NBX® Administrator's Guide

V3000 Analog
V3000 BRI
V3001R
V5000
NBX 100

Release 6.0

Part Number 900-0212-01 AA
Published August 2006

http://www.3com.com/

3Com Corporation
350 Campus Drive
Marlborough, MA
01752-3064

CONTENTS

5 TELEPHONE CONFIGURATION

7 CALL DISTRIBUTION GROUPS

8 PSTN GATEWAY CONFIGURATION

16 NETWORK MANAGEMENT

B ISDN Completion Cause Codes

C Configuring Option 184 on a Windows 2000 DHCP Server

D ConneXtions H.323 Gateway

About This Guide

This guide describes how to configure and manage NBX® Networked Telephony Systems. For information about how to install an NBX system for the first time, see the *NBX Installation Guide*.

If the information in the release notes differs from the information in this guide, follow the instructions in the release notes. Release notes are available on the NBX Resource Pack DVD.

How to Use This Guide

Table 1 can help you find information in this guide.

Table 1 Overview of This Guide

An overview of the systems	Chapter 1
Configure system settings	Chapter 2
Configure system features	Chapter 3
Maintain the system	Chapter 4
Configure telephones	Chapter 5
Configure user settings	Chapter 6
Configure Automatic Call Distribution	Chapter 7
Configure and manage digital and analog line cards	Chapter 8
Configure NBX Voice Messaging (voice mail), Auto Attendant, and Voice Profile for Internet Mail (VPIM)	Chapter 9
Enable and configure Session Initiation Protocol (SIP) operation	Chapter 10
Prepare and configure the dial plan	Chapter 11
Configure Virtual Tie Lines and TAPI Rout Points	Chapter 12
Download optional software and the LabelMaker utility	Chapter 13
Licensing and upgrade information	Chapter 14
Create reports	Chapter 15
Configure SNMP, Syslog, event logging and maintenance alerts	Chapter 16
Install and configure international language settings	Chapter 17

Table 1 Overview of This Guide

Troubleshooting information	Chapter 18
Third-party messaging system	Appendix A
ISDN Completion Cause Codes	Appendix B
Option 184 on a Windows 2000 DHCP server	Appendix C
3Com ConneXtions software	Appendix D
Caller ID behavior	Appendix E
Telephony and networking terms	Glossary
References to all topics in this book	Index
FCC and Industry Canada information, Software End-User License Agreement, and Limited Warranty for Software and Hardware	page 579

Conventions

Table 2 lists conventions that are used throughout this guide.

Table 2 Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, device, system, or network.
	Warning	Information that alerts you to potential personal injury.

International Terminology

Table 3 lists the United States and international equivalents of some of the specialized terms that are used in the NBX documentation.

Table 3 International Terminology

Term used in U.S.	Term used outside the U.S.
Toll restrictions	Call barring
Pound key (#)	Hash key (#)
CO (central office)	Telephone Exchange
Toll-free	Free-phone
Analog Line Card	Analog Trunk Line Interface Module

Your Comments

Your suggestions are important to us. They help us to make the NBX documentation more useful to you.

Send comments about this guide or any of the 3Com NBX documentation and Help systems to:

`Voice_TechComm_Comments@3com.com`

Please include the following information with your comments:

- Document title
- Document part number (found on the front page)
- Page number

Example:

NBX Administrator's Guide

Part Number 900-0212-01 Rev AA

Page 25

As always, address all questions regarding the hardware and software to your authorized 3Com NBX Voice - Authorized Partner.

1 INTRODUCTION

The *NBX Administrator's Guide* explains how to configure your NBX® system. This chapter describes these topics:

- Network-based Telephony
- NetSet Administration Utility

For information about how to install hardware components, see the NBX Installation Guide.

Network-based Telephony

3Com Networked Telephony Solutions merge telephony with networking by delivering business telephone service over a data network.

To a telephone user, a 3Com Telephone is an office telephone. You can use it to make and receive calls, transfer calls, park calls, use voice mail, and so on. Inside, the 3Com Telephone is a network device that can communicate over the LAN using Ethernet frames or IP packets. The telephone also includes a LAN port. You can connect your computer to your network through the telephone and avoid the need for a second LAN connection at the desktop.

The core of the system is the *Call Processor*. The Call Processor manages the processes of making and receiving calls, providing voice mail and Auto Attendant services, and responding to requests for special services, such as access to the NBX NetSet administration utility, Computer Telephony Integration (CTI) services, or the system's IMAP (Internet Message Access Protocol) server.

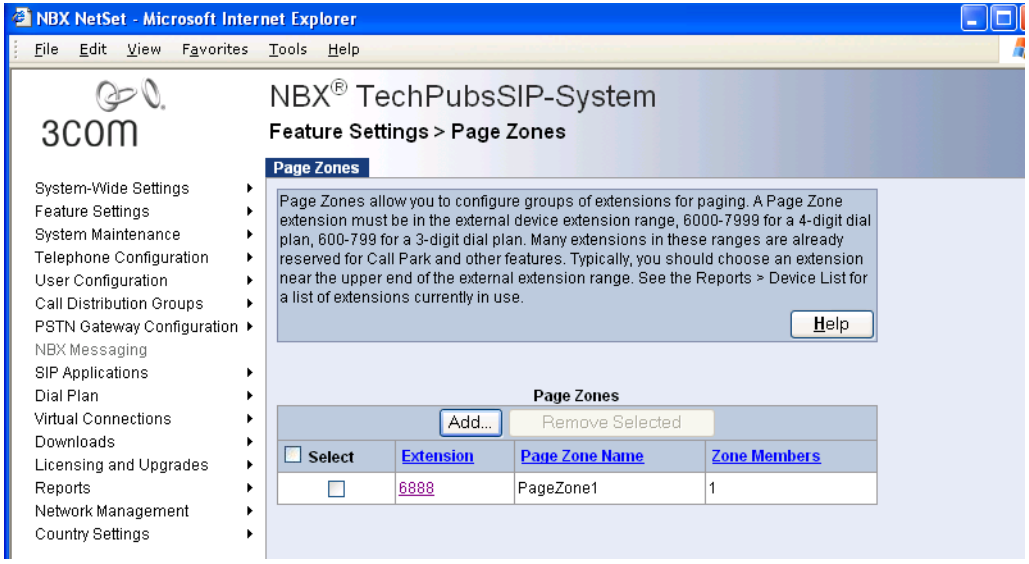
NetSet Administration Utility

the NBX NetSet utility is a browser-based interface that you use to configure and manage the system. the NBX NetSet utility requires any of these browsers:

- Microsoft Internet Explorer 5.5 or higher
- Netscape Navigator 7.0 or higher
- Mozilla Firefox 1.0 or higher

Figure 1 shows a sample NetSet window. The navigation menu is on the left of the window. Place the cursor over any of the functions to expand the view of that function and display all the associated options.

Figure 1 NetSet Utility - Page Zones Window

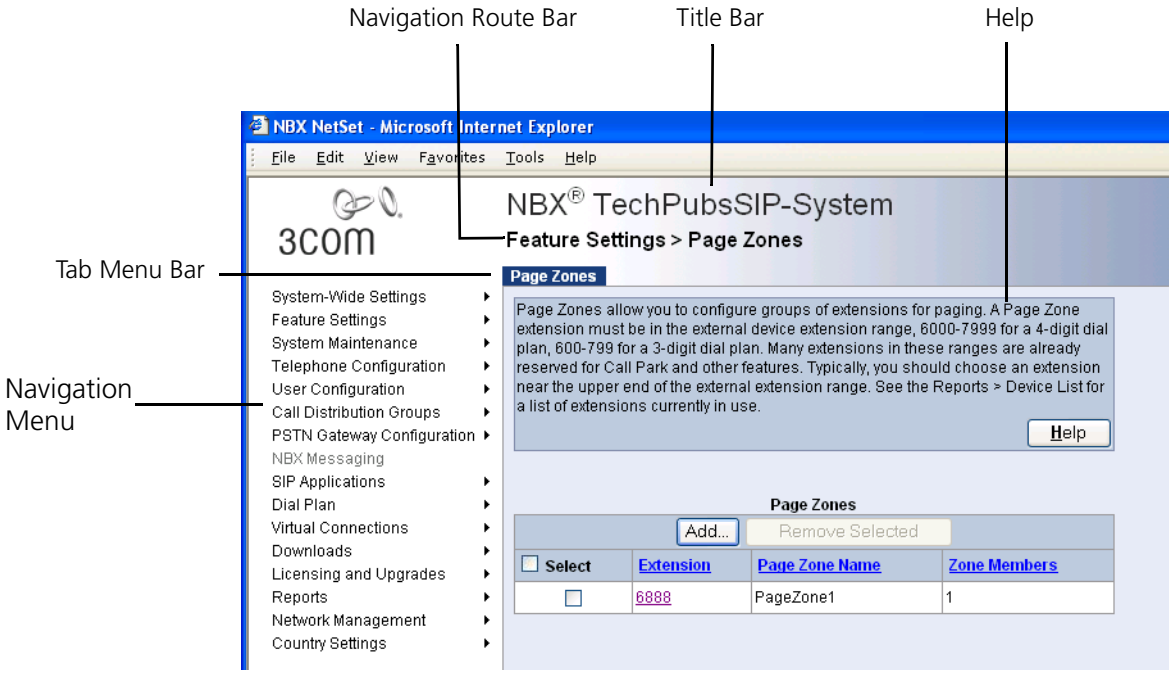


Systems present the NBX NetSet utility through an embedded web server that is integrated in the system software. NetSet passwords grant system administrators and telephone users different levels of access privileges. Individual telephone users can view or change their personal settings, such as personal speed dial lists, off-site notification settings, and ringing tones. System administrators can manage user profiles and devices, change system parameters, such as dial plan settings, and upgrade the system software.

NetSet User Interface

Figure 2 shows the NBX NetSet utility user interface. Each NetSet user interface page contains common elements.

Figure 2 User Interface Elements



- Title Bar — The NBX trademark followed by the system (host) name.
- Navigation Route Bar — The current page location, which is the selected navigation menu item and the selected submenu item.
- Navigation Menu — A list of all navigation groups in the NBX NetSet user interface. The navigation menu is partially or fully disabled under certain conditions. These conditions include:
  - System backup in progress: All menus are disabled.
  - System restore in progress: All menus are disabled.
  - System shutdown: All menus are disabled.
  - No system license: Only *Licensing and Upgrades* and *System Maintenance* menus are enabled.
- Tab Menu Bar — Displays when you click a menu item or submenu item, or when you click a link to a record.
- Help — Quick help text plus a button that invokes detailed help.

2 System Settings

This chapter provides information about how to configure settings, whose effects span the entire system, and includes these topics:

For more information about these topics and configuration procedures, see the online Help.

Auto Discovery

The Auto Discovery feature simplifies initial system configuration by adding information about new devices to the configuration database. *Devices* include telephones, Analog Line Card ports, Digital Line Card channels, Analog Terminal Adapter ports, 3Com Attendant Consoles, and *virtual devices,* such as the pcXset Soft Telephone and the ConneXtions H.323 Gateway. Devices must have network connectivity with the Call Processor.

After the system discovers a device, the Auto Discovery process does not find that device again. To remove a device from the system database, use the NBX NetSet utility to remove the device and its database record manually. Note that if you delete a telephone user, the system does not delete the device associated with that user.

The system does not discover licensed devices until you enter the appropriate Group License. For more information about Group Licensing, see the NBX Installation Guide.

Table 4 summarizes Auto Discovery actions for system components.

Table 4 Auto Discovery Actions on System Components

Component	Auto Discover Action
Analog Line Card and V3000 analog line ports	Gathers configuration information from each port on the card, assigns a default extension, and enters the information into the configuration database.
Digital Line Card	Gathers configuration information from the card, assigns a default extension, and enters the information into the configuration database. After you Auto Discover the Digital Line Card, you might need to edit the dial plan to configure Direct Inward Dial (DID) numbers.
3Com Telephones Analog Terminal Cards Analog Terminal Adapters V3000 ATA port	Gathers configuration information from the telephone, assigns a default User Profile labeled *new user*, assigns the next lowest available extension number to the profile, and enters the information into the configuration database. Auto Discover Telephones finds both Analog Terminal Cards and Analog Terminal Adapters. By default, the Auto Discover process assigns extension number 1000 (4-digit dial plan) or 100 (3-digit dial plan) as the first telephone extension. You can use the NBX NetSet utility to specify a new extension starting number. To simplify Auto Attendant configuration, start a range at a base number, for example, 1000/100, 2000/200, 3000/300, or 4000/400. The default Auto Attendant assumes that extension 1000 (4-digit dial plan) or 100 (3-digit dial plan) is the extension of a human attendant (receptionist).
3Com Attendant Console	Finds and configures any installed 3Com Attendant Consoles. The system maps the first 100 existing telephones, except for the extension that is associated with the Attendant Console, to Attendant Console buttons. The lowest extension is automatically associated with the Attendant Console. Typically, you enable Auto Discover Attendant Consoles after you have installed all your telephones.
pcXset Soft Telephone	Enables the Auto Discover feature on installations of the pcXset PC Telephone Client when the following conditions are true: ■ The pcXset PC Soft Telephone program is running on the host PC. ■ The pcXset PC Soft Telephone host computer is connected to the network. ■ You have entered the proper license key into the NBX NetSet utility.
ConneXtions H.323 Gateway	Configures line card port settings when the following conditions are true: ■ The ConneXtions H.323 Gateway program is running. ■ The ConneXtions H.323 Gateway host computer is connected to the network. ■ You have entered the proper license key into the NBX NetSet utility.

Initial System Configuration

To use the Auto Discover feature for initial system configuration:

1. Log in to the NBX NetSet utility using the administrator username and password.
2. Click *System-Wide Settings* > *Enable Features System-Wide*.
3. Verify that the *Extensions Start At* field is set to what you want, and then click *Apply*.

   For a 4-digit dial plan, extensions start by default at 1000. For a 3-digit dial plan, extensions start at 100.

   Do not specify a starting extension that begins with zero (0), which will cause the Auto Discover process to fail.
4. Click *System-Wide Settings* > *Auto Discovery*.
5. Select the check box for the device type that you are configuring and click *Apply*.

   3Com recommends that you Auto Discover one device type at a time. See the online Help for detailed information about each field.

Auto Discovery Notes

- If devices are on a different subnet from the Call Processor, enable IP on the Call Processor (*System-Wide Settings* > *IP Settings),* and each device must have IP configuration information.
- You can use DHCP to configure the telephones. You must configure the DHCP server to provide the Call Processor IP address through option 184. Also, you can use the keypad to program IP settings into each device. See "Configuring Option 184 on a Windows 2000 DHCP Server" on page 457 for DHCP information and "Using the Telephone Local User Interface Utility" on page 413 for telephone local programming instructions.
- The Auto Discovery and software download processes might take a few moments to complete. The Call Processor initializes devices one at a time. If you have connected many new devices to the system at the same time, the Auto Discovery process requires more time.
- A fully initialized telephone displays its extension and the date and time. If there are no extensions available, the Auto Discover process fails, and the telephone's display panel continues to display the telephone's MAC address.

- If you are adding devices that do not have a display panel, such as 3100 Entry Telephones, connect the devices one at a time and then refresh the *Telephone Configuration* > *Telephones* list after you connect a device to see the extension assigned to that device.
- If you are installing a 3Com Attendant Console, connect it *after* you have discovered all of the telephones. The Auto Discover Attendant Consoles process maps all existing telephone extensions to the Attendant Console.

Disabling the Auto Discovery Feature

After you finish the Auto Discovery process for the initial configuration, disable Auto Discovery so that the Call Processor does not continue to search for added devices.

To disable the Auto Discovery feature:

1. Log in to the NBX NetSet utility using the administrator username and password.
2. Click *System-Wide Settings* > *Auto Discovery*.
3. Clear all *Auto Discover* check boxes.
4. Click *Apply*.

Enable Features System-Wide

From the System-Wide Setting page, you can make changes to these settings.

- Extensions Start at
- External Prefix
- RTP DTMF Payload Type
- Caller ID Wait Timer
- External Paging Delay
- External Page Alert Volume
- Handsfree on Internal Transfer / Camp On
- Handsfree on External Transfer / Camp On
- System-wide CLIR
- One Button Transfer
- Pulse Dialing
- Supervisory Monitoring

- Call Timer
- Music On Hold
- Music on Transfer
- NBX Messaging
- IP Messaging or Third-Party Messaging
- URL for user access to IP Messaging or third-party messaging
- Enable SIP

To configure system-wide settings:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *System-Wide Settings* > *Enable Features System-Wide*.
3. See the online Help for detailed information about the settings and how to modify them.

How Call Timer Works With Other Telephone Features

Table 5 summarizes how Call Timer works with other PBX-type features.

Table 5 Call Timer Behaviors

Feature	Description
Internal Call	The call duration displays on the originating telephone when the telephone user finishes dialing the destination number. The call time increments while the called number is ringing. Call Timer does not work if the caller enters an invalid internal extension.
External Call	Call Timer behavior for an external call is the same as that of an internal call except in these cases: ■ If the caller enters an invalid external number ■ If the telephone of the called number is busy In these cases, the call time continues to advance.
Hold	When you put a call on hold, the system hides the Call Timer display. However, the Call Timer count continues to increment during the time that the call is on hold. When you take the call off hold, the Call Timer reappears.

Table 5 Call Timer Behaviors

Feature	Description
Transfer	When you transfer a call, the Call Timer count does not carry forward to the transfer destination. However, during the time period that the call is ringing on the transfer destination telephone, the Call Timer count continues to increment on your telephone. When the telephone user to whom you transferred the call answers the call, that user sees the Call Timer count start from zero.
Conference Call	The Call Timer value on the telephone that originated the call increments from the time at which the call originated. The Call Timer value on each telephone that is added to the conference increments from the time the conference participant answered the phone. If the conference originator drops other parties in the conference and stays with one party at the end, the Call Timer is based upon the total time the two parties spent in on the call, including any time before or during the conference.
Call Park	Call Park behavior is similar to the Transfer feature. However, if the telephone that unparks the call is the same telephone that parked the call, Call Timer displays the total time based on the time when the telephone originated the initial call.
Transfer Through Auto Attendant	If the caller dials the main Auto Attendant number, and the Auto Attendant transfers the call to the extension of choice (or to the default destination), then the called party sees the same behavior as if the call had been transferred. That is, the Call Timer count at the transfer destination starts when the called party answers the call.
Bridged Calls	For bridged calls, the Call Timer display depends on the off-hook indicator. **Example**: An administrative assistant answers the phone, and puts the call on hold. Then, the a site manager picks up the call. The manager sees the counter start from zero. However, if the administrative assistant puts the call on hold and retrieves it later, then the administrative assistant sees that the system has defined the Call Timer display for normal hold. **Example**: An administrative assistant puts a call on hold, and the manager picks up the call and then puts it on hold. Then, the administrative assistant picks up the call. In this case, the administrative assistant sees the Call Timer display as if the administrative assistant had picked up a new call.

System Identity

The System Identity window shows the current system settings, such as the software version, the IP address of the system, and the amount of free memory. To view system settings:

1 Click *System-Wide System Settings* > *System Identity*.

Table 6 describes the System Settings fields.

Table 6 System Settings

Field	Purpose
Software Version	The call control software for the system.
System Serial #	The serial number on the Call Processor circuit board.
Host Name	This is an IP setting. It is a name you can give to the system so you do not have to specify the IP address when you access the NBX NetSet utility through a browser.
IP Address	The IP address of the system.
Default Gateway	The IP address of the destination host for any IP packet not addressed to a host on the local subnetwork.
Subnet Mask	An IP setting that identifies the network and host portions of an IP address on the network.
Network Protocol	The transport mechanism for voice packets. *Ethernet only*: All communications are at the Ethernet frame layer. *Standard IP*: IP communications are used for traffic between NBX system addresses. Every device needs an IP address. *IP On-the-Fly*: An implementation of IP communications in which Layer 2 (Ethernet) devices temporarily use a Layer 3 (IP) address only when those devices need to communicate with a Layer 3 device on a different subnetwork. The system administrator defines an address pool that assigns the IP address. After the Layer 2 device returns to the idle state, the IP address returns to the pool of available addresses for future use.
System MAC Address	The hardware address of the system.
MOH MAC Address	The hardware address of the Music-on-Hold (MOH) device.
Free Memory	Available memory on the system.
Memory Upgrade Installed	Indicates whether this system has had a memory upgrade. Possible values are: ■ *Yes* (V3000, V5000 systems) ■ *No* (V3000, V5000 systems) ■ *N/A* (NBX 100, V3001R systems)

Table 6 System Settings (continued)

Field	Purpose
File System	The file system this system uses. ■ NBXFSV1 - The pre-release R6.0 file system. ■ NBXFSV2 - The newer file system that is shipped with release R6.0 or higher systems, which offers better performance and upgrade capabilities. If you upgrade an existing system to release R6.0, the system continues to use NBXFSV1.
Date and Time	The current system date and time. To modify, click *System-Wide Settings* > *Set Date and Time*.
System Start Time	The last time you initialized the system (boot time).

Business Information

You can configure information about the your business, such as business address and hours, including time of day service modes. You can also view the current mode and force the system into a different mode.

To enter business information:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *System-Wide Settings* > *Business Information*.
3. See the online Help for procedures to modify these types of information:
   - Business information
   - Business hours
   - System mode

   Click the Business Identity tab to display the information that you configure in the Business Information, Business Hours, and System Mode windows.

System Mode

The System Mode window lets you specify that the system operate in a particular mode or automatically. If necessary, you can force the system into a specific Time of Day Service mode without changing other system settings, such as Business Hours. If the system is in Automatic mode, it constantly compares the current time of day and day of week with the settings you establish in the Business Hours window (click *System-Wide Settings* > *Business Information* and click the Business Hours tab).

Business Hours

The Business Hours window allows you to define business hours for three separate service modes: *Open*, *Lunch*, and *Other*. Any time period that does not fall within these specified hours is considered *Closed*. Business hours link directly to time-of-day service modes and can affect other settings in the system, such as the Auto Attendant.

If the system mode is set to Automatic, the system constantly compares the current time of day and day of week with the business hour tables. The system knows the current day of the week and proceeds across the tables in a sequential manner, looking for business hours that match the current time of day. The system examines the three tables sequentially: first the Other mode, then the Lunch mode, and then the Open mode. The system moves across the tables until it finds a match. It skips a blank table.

Date and Time

The Date and Time window allows you to configure the following:

- System Date and Time
- Simple Network Time Protocol (SNTP)

System Date and Time

Make sure the system date and time are accurate because it affects these system features:

- The 3Com telephone display panel
- Business hours behavior
- Time-dependent prompts in the Auto Attendant
- Time and date stamp on voice mail

To access the date and time settings in the NBX NetSet utility:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *System-Wide Settings > Date and Time.*
3. See the online Help for the procedure to set the system date and time.

If you enter the system time and select a new time zone simultaneously, (that is, you do not apply the system time first) the system automatically adjusts the system time you entered to correspond to the selected time zone. For example, if the system time is set to 6:00 AM US Pacific, select the US Pacific time zone and allow the system to adjust the time

automatically. If you enter 6:00 AM and then select the US Pacific time zone, the system adjusts the system time based on 6:00 AM and displays the system time as 3:00 AM US Pacific.

Simple Network Time Protocol (SNTP)

The Simple Network Time Protocol (SNTP) synchronizes CPU clocks across the Internet. SNTP belongs to the TCP/IP suite and works at the Application layer in the OSI model, and uses UDP port 123 for communication. SNTP Version 4 can operate in either unicast (point to point), multicast (point to multipoint), or any cast (multipoint to point).

If you need to coordinate your system time with other Internet devices, use the NBX NetSet utility to synchronize the system to an SNTP server at a specified interval.

The initialization process initializes the SNTP client and connects to an available SNTP server. The SNTP server provides the time, which the system uses. When the synchronization interval expires, the system synchronizes with the SNTP server again. Any changes to the SNTP configuration take effect when the synchronization interval expires.

The system uses the time provided by the SNTP server for all references to local time. This includes the time stamps used by the Call Processor, phones, and gateways.

If the SNTP server fails, you can configure the system to transfer server control to another active SNTP server in the list. (You have the option to identify up to three SNTP servers to the system).

See the online Help for information about the procedure to configure the system to use SNTP.

IP Settings

The IP Settings window allows you to define the network protocol settings for this system and, if you are using IP On-The-Fly, to define the range of IP addresses that the system can use to assign addresses to devices as needed.

Before you configure the IP settings, you must have all necessary network information, such as the network protocol, VLANs, Layer 3 IP information about this Call Processor, and any DNS server addresses. This information is propagated in the IP Settings window.

The IP Address Ranges window allows you to add or delete a range of IP On-the-Fly addresses.

Audio Settings

Audio Settings enable you to affect the network impact of your audio packets by enabling or disabling compression and silence suppression. You can enable and disable these settings for the entire system and then override the system-wide setting for individual devices.

Compression Overview

Before voice traffic can be transmitted over a digital network, the audio waveform, an analog signal, must be encoded into a digital format. The digitized audio is packetized and delivered over the network to a destination, and then decoded back into a voice waveform. Software called a codec (coder/decoder) converts the audio information between digital and analog formats.

Digitized audio formats have different properties. Each format represents a compromise between bandwidth and audio quality, that is, high quality audio typically requires more network bandwidth. Compressing the digitized audio data can conserve bandwidth with little compromise in audio quality, but compression requires increased processing overhead when encoding and decoding the audio information. Too much processing overhead can introduce delay.

Table 7 lists the codecs that the system supports and describes the characteristics of each one.

Table 7 Supported Codecs

Codec	Description
G.711 No Compression	An International Telecommunications Union (ITU) standard for audio encoding. Encoding and decoding is fast and support is widespread. Also called *MULAW* or *µLAW*. *A-law* is a slight variation, which European telephone systems use. G.711 provides high quality audio at 64 kbps. Telephone companies worldwide use G.711 encoding to provide "toll-quality audio."
ADPCM Medium Compression	Adaptive Differential Pulse Code Modulation (ADPCM) provides good quality audio at a lower bitrate (32 kbps) than G.711. The system uses the International Multimedia Association (IMA) version of ADPCM.
G.729 High Compression	G.729, an ITU standard, employs a more sophisticated compression technique than ADPCM and it is supported worldwide. The G.729A codec compresses the audio information to 8 kbps, although processing overhead results in actual bandwidths greater than 8 kbps.

Table 7 Supported Codecs

Codec	Description
G.722 G.722.2 G.722.2LB	G.722.2 is an ITU-T standard for wideband voice applications and services. G.722.2 is an adaptive multi-rate wideband codec that uses bit rates ranging from 6.6 to 23.85 kbps.
Wideband Audio	G.722 is an SB-ADPCM (sub band Adaptive Pulse Code Modulation) codec. It runs ADPCM on both the low band (0 - 4000 Hz) and the high band (4000 - 8000). The raw bit rate (without network packet headers) is 64 kbps.
	G.722.2 is a CELP (code excited linear prediction) based codec. G.722 is a 23.85 kbps rate. G.722.2 LB has a rate of 8.85 kbps. The standard was originally designed for wireless networks and the different rates allow for adapting to varying channel conditions.

Codec Selection

It is important to remember not to select a codec based on compression alone. Consider the trade-off between audio quality and bandwidth use.

System-Wide Audio

For system-wide audio, base the default list order on audio quality:

Table 8 Default Order List Based on Audio Quality

Codec	Quality	Bandwidth
G.722.2	**best quality**	medium bandwidth
G.722	**high quality**	high bandwidth
G.711	**good quality**	high bandwidth
G.722.2LB	**good quality**	low bandwidth
G.729	**medium quality**	low bandwidth
ADPCM	**low quality**	medium bandwidth

VTL Calls Audio

For Virtual Tie Line (VTL) audio, base the default list order on bandwidth usage:

Table 9 Default Order List Based on Bandwidth Usage

Codec	Quality	Bandwidth
G.722.2LB	good quality	**low bandwidth**
G.729	medium quality	**low bandwidth**

Table 9 Default Order List Based on Bandwidth Usage

Codec	Quality	Bandwidth
G.722.2	best quality	**medium bandwidth**
ADPCM	low quality	**medium bandwidth**
G.722	high quality	**high bandwidth**
G.711	good quality	**high bandwidth**

Custom Audio

For custom audio that you determine based on the needs of your site, you can choose the list order:

Table 10 Default Order List Based on Bandwidth

Codec	Quality	Bandwidth
G.729	**medium quality**	**low bandwidth**
G.722.2	**best quality**	**medium bandwidth**
ADPCM	low quality	medium bandwidth
G.722.2LB	good quality	low bandwidth
G.722	high quality	high bandwidth
G.711	good quality	high bandwidth

For the audio settings that are configured on each device, 3Com provides sorted lists such as these. Each list contains the codecs supported for that device only.

For example, a default codec configuration list for a 3Com Business Telephone (that is, sorted by audio quality) might show a codec configuration list like the following:

G711	good Q	high BW
ADPCM	low Q	med BW

If you have set device options for a low bandwidth connection, then the 3Com Business Telephone codec configuration list might show:

ADPCM	low Q	med BW
G711	good Q	high BW

When the system negotiates which codec to choose, the process starts from the top of the list and queries devices to discover if they support the codec. If the device is supported, the system chooses the codec; otherwise, the system goes on to the next codec in the list and initiates the query process.

Codecs and NBX Devices

Codecs reside on the NBX devices — telephones, analog terminal adapters, and so forth. Some older devices do not support the latest codecs. Therefore, during call setup, NBX devices negotiate an encoding scheme that both devices (or all devices on a conference call) support.

Table 11 lists each device that must encode or decode audio, and shows how each device supports the available codecs. Certain devices are marked "N/A" for the G.722 codecs because those codecs are for wideband audio, which is not supported by wide area networks or across the PSTN.

Table 11 Audio Encoding Supported by NBX Devices

Device	Part Number	G.729	ADPCM	G.711	G.722	G.722.2	G.722.2LB
3Com 1102, 2102, and 2102-IR Business Telephones	3C10121 3C10122 3C10226A 3C10228IRA	No	Yes	Yes	No	No	No
	3C10226PE 3C10226B 3C10228IRPE 3C10228IRB 3C10281PE 3C10281B	Yes	Yes	Yes	No	No	No
3Com 2101 Basic Telephones	3C10248PE 3C10248B	Yes	Yes	Yes	No	No	No
3Com 3100 Entry Telephone	3C10399A	Yes	Yes	Yes	No	No	No
3Com 3101, and 3101SP Basic Telephones	3C10401A 3C10401SPKRA	Yes	Yes	Yes	No	No	No
3Com 3101B Basic Telephone	3C10401B	Yes	Yes	Yes	Yes	Yes	Yes
3Com 3101SPB Basic Telephone	3C10401SPKRB	Yes	Yes	Yes	Yes	Yes	Yes
3Com 3102 Business Telephone	3C10402A	Yes	Yes	Yes	No	No	No
3Com 3102B Business Telephone	3C10402B	Yes	Yes	Yes	Yes	Yes	Yes
3Com 3103 Manager's Telephone	3C10403A	Yes	Yes	Yes	Yes	Yes	Yes
3Com 3106C and 3107C Cordless Telephones	3C10406C 3C10407C	Yes	Yes	Yes	No	No	No

Table 11 Audio Encoding Supported by NBX Devices (continued)

Device	Part Number	G.729	ADPCM	G.711	G.722	G.722.2	G.722.2LB
3Com 3108 Wireless Telephone	3C10408A	Yes	Yes	Yes	No	No	No
Analog Terminal Adapter	3C10120 3C10120B	No	Yes	Yes	N / A	N / A	N / A
	3C10400	Yes	Yes	Yes	N / A	N / A	N / A
Analog Terminal Card	3C10117 3C10117B-INT	No	Yes	Yes	N / A	N / A	N / A
	3C10117C	Yes	Yes	Yes	N / A	N / A	N / A
Analog Line Card	3C10114 3C10114-ANZ	No	Yes	Yes	N / A	N / A	N / A
	3C10114C	Yes	Yes	Yes	N / A	N / A	N / A
Digital Line Card	3C10116, 3C10116B 3C10116C 3C10164-ST (BRI) 3C10164C-ST (BRI) 3C10165 3C10165C	No	Yes	Yes	N / A	N / A	N / A
	3C10116D 3C10165D	Yes	Yes	Yes	N / A	N / A	N / A

Silence Suppression Overview

Silence suppression is a method of reducing the number of packets transmitted during a conversation. Silence suppression can help you avoid dropped packets on a congested network. During a conversation there are periods of silence. A packet of silence takes up as much bandwidth as a packet with audio data. If you enable Silence Suppression, the telephone sends a *silence indicator* when it senses the start of a silent period and it suppresses all subsequent voiceless frames. When another NBX device receives this indicator, it generates and inserts white noise until it receives the next frame that contains audio data. If you enable Silence Suppression, a careful listener might notice a difference in audio quality. The background white noise generated by the receiving telephone is subtly different from the silence in an audio stream.

Silence suppression results in compromises to audio quality. Do not enable suppression unless you are trying to solve network bandwidth congestion issues that you cannot solve through other means, such as increasing network capacity.

To enable Silence Suppression, click *System-Wide Settings* > *Audio Settings*.

Timers

System timers enable you to set time-out periods for the system features that are described in Table 12.

To set timers:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *System-Wide Settings* > *Timers.*

Table 12 System Timers

Field	Purpose
Forward Voice Mail On Timeout	When a telephone's Forward to Mail feature is *enabled*, sets the duration of ringing before the system forwards a call to voice mail. **NOTE:** If you set this time to be less than six seconds, Caller ID information is not captured in voice mail.
Forward Voice Mail Off Timeout	When a telephone's Forward to Mail feature is *disabled*, sets the duration of ringing before the system forwards a call to voice mail. The system uses this setting as the default for each new telephone user that you add to the system. If you modify this value, users added after the change use the new value as the default. Telephone users added prior to the change are unaffected. Individual telephone users can modify the default setting in the *Call Forward* window of the User interface of the NBX NetSet utility by specifying the number of times the telephone rings before the system forwards a call.
Line Port Hold Timeout	For a call that originated on an outside line, the length of time that the call remains on hold before it rings at the extension that placed the call on hold.
Call Park Timeout	The length of time that a call can be parked before it rings at the extension that parked the call.
Conference Timeout	The length of time before the system abandons a conference attempt. Applies to a blind conference only. The timeout takes effect under these conditions: ■ Two people, A and B, are involved in a call and one of them attempts to blind conference another person, C. ■ C does not answer and C's voice mail does not pick up the call. After the Conference Timeout period, the system stops ringing C's telephone, stops attempting to conference with C, and reverts to the call between A and B.
Transfer Timeout	The length of time that a transferred call attempts the transfer before it rings at the extension that transferred the call.

Table 12 System Timers

Field	Purpose
TAPI Line Redirect Timeout	The length of time before a call redirected from a TAPI route point by an external application returns to its original destination. After two failures, the call goes to the TAPI route point's call coverage option. TAPI Line Redirect allows an external TAPI application, typically a call center application, to reroute incoming calls based on caller ID information automatically. For more information, see TAPI Route Points.
Camp On Timeout	The length of time that a call can camp on a busy extension before the system returns the call to the extension that initiated the Camp On feature. The Camp On Timer can be set in increments of 10 seconds. The default value for Camp On Timer is 180 seconds. The maximum value that you can set the timer for is 600 seconds.
Automatic Callback Timeout	The length of time that a call can be designated for call back before the system cancels the call. The Callback Timer has default value of 12 hours. You can set the timer to have a null value. If Automatic Callback is not returned in the specified time, Automatic Callback is cancelled. A system reboot also cancels the Automatic Callback on an extension.

Multicast Addresses

The system uses IP multicast addressing to distribute information for these system features, which are available on Layer 2 and Layer 3 IP devices:

- Mapped line appearances
- Internal pages
- External pages
- Conference calls

The Music on Hold (MOH) feature is available on Layer 2 devices only. The IP implementation uses Internet Group Management Protocol (IGMP) to transmit and distribute the necessary data and audio.

If you configure your system to use IP On-the-Fly or Standard IP and your switches use IGMP Snooping, you must have an IGMP Host on the network. Typically, an IGMP Host is an IP Multicast Router or a switch that has IGMP Query capability.

The system IGMP is an implementation of administratively scoped IP multicast that uses three scopes of administration:

- **Local scope** — Limited by local routers with IP addresses 239.255.0.0 through 239.255.0.16
- **Organizational local scope** — Limited by boundary routers with IP addresses 239.192.0.0 through 239.192.0.14
- **Global scope** — IP addresses 224.2.0.0 through 224.2.127.253

IGMP might not be available in all systems or network topologies. All routers between the various components must support IGMP and the necessary router protocols to establish a path for the IP multicast packets.

Each event that occurs in an IGMP setup, such as taking a telephone off the hook, causes a packet of 200 Kb to 300 Kb to be sent.

The default settings for the IP multicast addresses function in most network environments. Certain addresses are reserved.

The MAC address and the IP address displayed on any one line of the Multicast Address List *window are not related.*

There are two methods for selecting multicast addresses:

- **Change IP** — Lets you select a starting address for all entries. Changing IP multicast addresses is a quick way to change the range of system multicast addresses to avoid conflicts with other equipment on your network.
- **Change bins** — Lets you change a single entry by selecting from a list of available bins. Changing IP bins is useful for changing a single address that might conflict with another system device. Consult your network administrator to determine which address is in conflict and the new address to choose.

To change multicast addresses:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *System-Wide Settings > Multicast Addresses.*
3. See the online Help for more information.

3 Feature Settings

This chapter provides information about configuring the system to take advantage of system features. It describes these topics:

- Account Codes
- Call Pickup
- Call Park
- Page Zones
- Ring Patterns
- Supervisory Monitoring
- Speed Dials
- WhisperPage

For more information about these topics and configuration procedures, see the online Help.

Account Codes

Account codes are additional numbers that telephone users dial to associate calls with specific functions, sources, or destinations. For example, call center operations often employ account codes to associate calls made by Automatic Call Distribution (ACD) agents with their relevant accounts for tracking purposes. (See Chapter 7 in this guide for more information about ACD.) Telephone users enter an account code while placing a call or during a call.

Verifying account codes is a global configuration setting, while *enforcing* account codes is a per-Class of Service (CoS) setting. If the CoS setting enforces the account code for that particular type of call, a telephone user *must* enter an account code before the system routes the call.

The enforced account code does not apply to internal or emergency (911) calls.

Account codes range from two to sixteen digits. The system allows up to 5000 account codes.

The system maintains a centralized list of account codes that you can update, and can verify the account codes that telephone users enter against this list of account codes.

Account codes are classified by four operation modes, which determine how strictly to enforce account code usage for outgoing calls based on Class of Service criteria. See the Account Codes: Operational Modes section of this chapter for information about operational modes.

Feature Interaction

This section describes the ways in which account codes interact with other features.

Bridged Station Appearance

Only a primary telephone can originate a call. However, once the call is answered, either the primary or the secondary telephone can place the call on hold and take it off hold. The last account code that the primary or the secondary telephone entered overrides the account code for the call.

CO Flash

The system does not enforce account code entry for calls that you originate by means of a CO Flash. This means that you can receive a call, perform a CO Flash, and make an external call without entering an account code.

Conference

During the time that forced account code mode is enabled, you must enter an account code for each leg of a conference. The account code applies to the call leg, and not to the call from which the conference is initiated. After the conference is completed, an account code entered by any telephone user overrides the account code for the conference call.

Emergency Numbers

The system allows emergency numbers without an account code.

Call Forwarding

You cannot specify account codes as part of a forwarding number. If you forward a call while forced account code entry is enabled, the call is forwarded and you are not prompted to enter an account code. A side effect of this feature interaction is that an internal extension could be used to forward calls to an external number and thereby circumvent forced account code entry.

International Dialing

If you enabled Force mode and a timeout occurs after you have entered the minimum number of digits and are still dialing, the system prompts you to enter an account code. After you enter the account code, you can continue entering digits for the international number.

Paging

You can use Paging without entering an account code.

Call Park

If you entered an account code before you park a call, that call is preserved when you unpark it. You can unpark calls without entering an account code. You can enter a new account code after unparking the call.

Redial

Account codes are *not* stored as part of the redial digits (except on analog phones), even if you specified the account code as part of a speed dial operation. If outbound digits are redialed while forced account code mode is enabled, the system prompts you to enter an account code.

Speed Dial

Phones with programmable buttons and Attendant Consoles can use speed dial with account codes. From the User interface of the NBX NetSet utility:

- Configure a one-touch speed dial with an account code. Click *Directory* and then the One-Touch Speed Dial tab. Use the following format in the *Number* field:

  [888] + Account code + **#** + Outbound number

You must use brackets, which indicates that **888** is a feature code.

- Configure a personal speed dial with an account code. Click *Directory* and then the Personal Speed Dial tab. Supply the account code separately in the Account Code field.

For security reasons, the telephone's display panel does not display the account code during a speed dial. If the account code is valid, the display panel displays the account name.

Call Transfer

If you enable Forced mode, when you transfer a call, enter an account code before the second call is routed. After the transfer is complete, the account code entered on the *second* call leg also applies to the transferred call.

This means that the first call (prior to the start of transfer) can have account code XXX, the second call (prior to the completion of the transfer) can have account code YYY, and the transferred call has account code YYY.

VTL

Forced account code entry applies to all VTL calls.

Account Codes: Operational Modes

Before you configure account codes for your system, make sure you are familiar with the enforcement and verification mechanisms and how they affect your call operations.

Codes are classified by one of the these modes:

- Forced / Verified Mode
- Forced / Unverified Mode
- Unforced / Verified Mode
- Unforced / Unverified Mode

Forced / Verified Mode

In Forced / Verified mode, the system first forces the telephone user to enter an account code and verifies that the code is correct before routing an outgoing call. The system verifies the account code against a master list that you establish.

To place an outgoing call, dial the outbound number in either of the following ways:

- Outbound number + # + Account code + #
- **Feature** + **888** + Account Code + # + Outbound number

In the first instance, you might not know or remember that an account code is necessary and dial only the outbound number. In this case, the telephone prompts you to enter an account code after a short period of time.

If the account code is *valid*, the Feature Success tone plays and the system routes the call.

If the account code is *invalid*:

- On a telephone with a display panel, the display panel displays the invalid account code and prompts you to enter the account code again. After three unsuccessful attempts to enter the account code, you must start over by reentering the outbound number and account code.
- On a phone without a display panel, the telephone plays the Feature Error tone and you must reenter the entire digit sequence.

The system does not require account codes for emergency calls, such as 911, and immediately routes the calls.

During the call, you can enter another valid account code using the following format:

F+ 888 + Account_code + #

You can enter multiple account codes during a call; the most recently entered account code overrides the previously entered account code. In Verified account code mode, the newest account code only overrides the existing account code if it has been verified.

The account code and account name information is available in the Call Detail Reporting (CDR) data. To download the NBX Call Reports software, click *Download* > *Applications*. To enable CDR, click *System Maintenance* > *Call Report Settings*.

Enforcing account codes is applicable for outgoing external calls only.

Forced / Unverified Mode

Forced / Unverified mode is similar to Forced / Verified mode in that the system forces you to enter an account code. However, because the system does not verify the account code, the telephone either:

- Displays the account name associated with the code.
- Displays the text string `Unknown Account`.

In this mode, it is possible for you to enter an invalid account code and still proceed with the call.

The account code and account name information is available in CDR.

The system only forces the use of account codes on outgoing, external calls.

Unforced / Verified Mode

In Unforced / Verified mode, the system does not force you to enter an account code. However, if you do enter an account code, the system verifies that the account code is correct.

You can enter an account code during the call using the following format:

Feature + **888** + Account_code + #

The system verifies the account code against the list of valid account codes.

- On a telephone with a display panel, an invalid account code shows the text string `Unknown Account`, and the call continues.
- On a telephone without a display panel, an invalid account code plays the Feature Error tone, and the call continues.

Unforced / Unverified Mode

Unforced / Unverified mode is similar to Unforced / Verified mode, but the system does not verify the account code. The telephone displays the account name if the account code is valid and the call continues.

The account code and account name information is available in CDR.

Configuring Enforcement and Verification

To enable or disable verification of outgoing calls:

1. Log in to the NBX NetSet utility using the administrator login ID and password.
2. Go to *Feature Settings* > *Account Codes*.
3. Enable the check box next to the appropriate account code (or create a new one before proceeding).
4. Enable or disable the *Enforce account codes verification* check box, as appropriate.
5. Click *Apply*.

To enforce or relax the need for an account code:

1. Log in to the NBX NetSet utility using the administrator login ID and password.
2. Click *User Configuration* > *Class of Service*.
3. Click the appropriate CoS Group name, which displays the Modify window.
4. Locate the appropriate Class of Service (such as International or Long Distance), then enable or disable the corresponding *Force Acct Code* check box.
5. Repeat the previous step for each appropriate Class of Service.
6. Click *Apply* to activate the changes and leave this window open, or click *OK* to activate the changes and close this window.

Call Pickup

Call Pickup allows telephone users who hear a telephone ringing to answer the call on their own telephones. To enable this feature, you add telephone extensions to Call Pickup Groups.

The Call Pickup feature is not supported for hunt groups. However, it is supported for ACD groups.

Group Numbers

Table 13 summarizes the Call Pickup group numbers.

Table 13 Call Pickup Group Numbers

System	Group Numbers
V3000, V3001R, V5000	50 Call Pickup groups: ■ Group 0 through group 31 (extension 500 through 531) ■ Group 32 through group 49 (extension 482 through 499) 50 Directed Call Pickup groups (extension 540 through 589)
NBX 100	32 Call Pickup groups from group 0 (extension 500) through group 31 (extension 531) 10 Directed Call Pickup groups from 540 through 549

See the NBX Telephone Guide *for user instructions about how to use Call Pickup.*

If you select *Auto Add Phones to Call Pickup Group 0* (*System-Wide Settings* > *Auto Discovery*), every telephone that you add to the system is a member of Call Pickup group 0 (extension 500). Any telephone can pick up calls to a telephone user who is a member of default Call Pickup Group 0. Telephone users can add or remove their own telephone extensions from the group to allow or prevent others from picking up their calls. See the *NBX Telephone Guide* and the User online Help for more information.

You can add telephone users to and remove them from any of the groups. Telephone users can remove themselves from Call Pickup group 0, but not from any other Call Pickup groups.

You can map Call Pickup Groups to user telephone buttons to provide one-touch access to the Call Pickup groups. See "Creating and Managing Button Mappings" in Chapter 5.

To configure call pickup groups and modify group membership:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *Feature Settings* > *Call Pickup*.
3. See the online Help for more information.

Call Park

When you park a call, anyone can retrieve it from any other telephone in the system by entering the Call Park extension that is associated with that call.

Example: You need to transfer an incoming call, but the person that you need to reach is not available. You can park the call on any unused Call Park extension, and then page the person and announce that Call Park extension. The person can then dial the Call Park extension from any internal telephone to retrieve the parked call.

These are the default system configuration extensions for Call Park:

- **4-digit dial plan:** 6000 through 6099
- **3-digit dial plan:** 601 through 609

Adding a Call Park Extension

To add a Call Park extension:

1. Click *Feature Settings* > *Call Park*.
2. Click *Add*.
3. Enter the number of an extension in the *Extension* field.
4. Enter a name for the extension in the *Name* field.
5. Click *OK*.

Changing a Call Park Extension Name

To change the name of a default Call Park extension:

1. Click *Feature Settings* > *Call Park*.
2. Click an extension.
3. Enter the new name for the Call Park extension in the *Name* field.
4. Click *OK*.

Removing a Call Park Extension

You can remove a Call Park extension at any time:

1. Click *Feature Settings* > *Call Park*.
2. Select the extension, or extensions, that you want to delete and click *Remove Selected*. To select all extensions, enable the *Select* check box.
3. Click *OK.*

To replace any extension that you remove, see "Adding a Call Park Extension" on page 53.

Page Zones

The Page Zone feature allows you to designate a subset of devices within the system as members of a zone. Telephone users then can page members of that group only, rather than paging all devices on the system. The system supports up to 16 page zones per system.

The system allows multiple simultaneous zone pages. However, a device that is currently paging or being paged will not respond to another page request.

A Page Zone extension must be in the external device extension range:

- 6000-7999 for a 4-digit dial plan
- 600-799 for a 3-digit dial plan

*The default 3- and 4-digit dial plans assign extension numbers that start with 7 as diagnostic. Diagnostics is a Class of Service that you can assign to a telephone user. For example, if you want to assign a page zone to extension 720, either change the dial plan (to make 7** an internal call) or assign the CoS permissions labelled Diagnostics to users who will be dialing the 720 page zone. To keep the dial plan and CoS defaults, use the extension range of 6000 – 6999 (or 600 – 699) for page zones.*

Many extensions in these ranges are already reserved for Call Park and other features. Typically, you choose an extension near the upper end of the external extension range. Click *Reports* > *Device List* for a list of extensions currently in use.

Page Zone Feature Support

The Page Zone feature supports the following features and desktop applications:

- Caller ID — The display panel on the device originating the zone page displays the zone page's name and extension; the recipients' display panels do not display the broadcaster's extension.
- Hands Free — A zone page reaches a device that has Hands Free enabled.
- Hold — A zone page reaches a device that has Hold enabled.

- Speed Dial (Personal) — A device is able to store personal speed dial extensions as zone page extensions.
- Speed Dial (System) — A device is able to store system speed dial extensions as zone page extensions.

All other features and desktop applications are not supported. A zone page does not reach a device that has Do Not Disturb enabled.

When zone paging, you cannot include devices from a different Call Processor in a local page zone. However, if your dial plan is configured to support Virtual Tie Lines (VTLs), you can include an extension on a different Call Processor in a zone page.

SIP telephones can neither initiate nor receive pages.

To configure Page Zones:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *Feature Settings* > *Page Zones.*
3. See the online Help for information about how to add, modify, and remove page zones.

Ring Patterns

You can set system-wide ring patterns, such as one, two, or three rings, to distinguish between internal and external calls.

Do not confuse ring patterns with ringer tones, which telephone users can set for their telephones from the NBX NetSet utility. For information about setting a telephone user's ringer tones, see the NBX Telephone Guides *or the* User online Help.

To set ring patterns:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *Feature Settings* > *Ring Patterns.*
3. See the online Help for more information.

Supervisory Monitoring

Supervisory Monitoring allows a supervisor to monitor calls on the system, with or without the knowledge of the parties engaged on the

call, as a part of the quality control operations of a site. Typically, you monitor or audit calls that are routed through ACDs, Hunt Groups, or TAPI Route Points. However, you can monitor any call.

This section describes these topics:

Introduction to Monitoring

Supervisory Monitoring takes place through domains. A *domain* is a collection of telephone users who are grouped because they are logically related in some way. In this case, the telephone users in a domain are candidates for monitoring. If you enable Supervisory Monitoring in a domain, each telephone user in that domain can be monitored.

By default, Supervisory Monitoring is disabled. You can enable or disable Supervisory Monitoring on a system-wide basis. Click System-Wide Settings > Enable Features System-Wide *and then enable the* Supervisory Monitoring *check box.*

There might be situations in which a telephone user's calls need not be monitored. In this case, the *Privacy List domain* is a special domain that contains telephone users whose calls cannot be monitored.

A monitoring session, in which an agent's call is actively monitored, includes:

- The supervisor, or monitoring party, who is any telephone user in the system who knows the Supervisory Monitoring domain password and thus can monitor the members of the domain associated with that password.
- The *agent*, who is any telephone user who is part of a supervisory monitoring domain and who a supervisor in that domain can monitor, unless that telephone user is in the Privacy List domain.

The actual audio state, or mode, of the session might be one of the following:

Table 14 Supervisory Monitoring Modes

Mode	Description
Monitor	Enables a supervisor to monitor a call with or without the knowledge of the agent or the external party (typically a customer).
Whisper	Enables a supervisor to coach or speak with an agent without the customer's knowledge.
Barge-In	Enables the supervisor to speak with both the agent and the customer.

You can configure announcement tones to allow the agent or the customer, or both, to know that the call is being monitored.

Domains and Upgrades

Supervisory Monitoring domains are a new feature in release R6.0. To create and manage Supervisory Monitoring domains, click *Feature Settings* > *Supervisory Monitoring* and see the online Help for more information.

If you upgrade to release R6.0 from a previous release, make sure you are aware of upgrade results.

Release R5.0 supported Supervisory Monitoring for calls that hunt groups, ACD groups, and route points managed. When you upgrade a release R5.0 system to release R6.0, the system creates new Supervisory Monitoring domains automatically for all existing groups for which the Supervisory Monitoring passwords were changed from the default setting. If a group's default password was not changed in release R5.0, the system does not create a new Supervisory Domain for that group.

The new Supervisory Monitoring domains have these characteristics:

- The upgrade process transfers all relevant information from release R5.0 groups to the new release R6.0 Supervisory Monitoring domains. For example, the members of a new Supervisory Monitoring domain are the same members of the Hunt Group or the ACD Group that you created in release R5.0.
- The name of each new Supervisory Monitoring domain that the system creates during the upgrade process is the group name plus the group number of the Hunt Group or the ACD Group that had Supervisory Monitoring enabled. The new password is the group's extension plus the former supervisory monitoring password. For

example, if ACD Group 4000 had password 1234 in release R5.0, the new Supervisory Monitoring domain password in release R6.0 is 40001234.

- The tones that are enabled for a new Supervisory Monitoring domain are the same tones that were in effect for the Hunt Group or ACD Group before the upgrade.
- The call type settings default to incoming group calls only.

Domains and Privacy

Be aware of the following privacy issues when you use Supervisory Monitoring on your system:

- **Monitoring Ability**

  A supervisor can monitor:

  - All call types, which includes incoming, outgoing, and non-ACD calls.
  - Anyone in the system.
  - Three-party conference calls. The supervisor counts as one of the parties in a conference, which supports up to four parties at one time.

- **Domains**

  A domain defines logical groupings of the agents who a supervisor, or supervisors, is required to monitor.

  The NBX 100 system can support up to 49 domains. All other hardware platforms can support up to 101 domains.

  Anyone who has a valid Supervisory Monitoring domain password can be the supervisor and monitor domain members.

Prior to release R6.0, the supervisor had to enter the extension and password of the last hunt group, ACD, or route point that the incoming call traversed to monitor a call. This restriction is removed.

You must create Supervisory Monitoring domains that specify the following information for the system:

- The Supervisory Monitoring domain's unique name and password
- The types of calls that the supervisor can monitor (Incoming Group Only calls or All calls)

- The calling groups (ACD, Hunt Group, or TAPI Route Point) that the supervisor can monitor
- The agents or telephone users than the supervisor can monitor
- Announcement tones for Monitor, Whisper, and Barge-In modes

- **Privacy List**

  The *Privacy List,* which is a reserved system domain, specifies those telephone users whom a supervisor cannot monitor. The Privacy List is unlike other Supervisory Monitoring domains:

  - You cannot change the name of the Privacy List.
  - You can define only telephone users for the Privacy List. There are no tone settings or call type settings for this domain.
  - You cannot add Hunt groups, ACDs, or TAPI Route Points as members of the Privacy List.
  - You can add members of the Privacy List to individual domains, even though these telephone users cannot be monitored. You can track these cases using reports.

- **Call Privacy**

  Call Privacy allows a telephone user to prevent a call from being monitored on a call-by-call basis. Telephone users can toggle Call Privacy on and off to block or accept monitoring.

  This contrasts with membership in the Privacy List domain, which ensures that a supervisor cannot monitor *any* calls associated with a telephone user.

  You can assign a telephone user to a CoS group that allows Call Privacy so that the telephone user can use Feature Code **428** to prevent the supervisor from monitoring the current call as follows:

  - The telephone user can activate the Call Privacy feature before a call (for example, by going off-hook and dialing Feature Code **428** and then dialing an internal or external call), or during a call (for example, by dialing Feature Code **428** after answering an incoming call). If the telephone user activates Call Privacy while on a call that the supervisor is monitoring, the monitoring session ends.
  - When an active Call Privacy session ends, (that is, the telephone user activates Call Privacy, initiates a call, and then exits the call) the Call Privacy settings are no longer applicable and the next call is open to monitoring.

You can map Feature Code **428** to one of the telephone system access buttons.

Announcement Tones and Supervisory Modes

This section describes information about the following topics:

- Supervisory Monitoring Announcement Tones
- Using Monitor Mode
- Entering Whisper Mode From Monitor Mode
- Entering Barge-In Mode From Monitor Mode
- Changing Agents and Changing Modes While Monitoring

The Call Timer feature on the display panel of the telephone does not work with Supervisory Monitoring. Also, to use Supervisory Monitoring, you must use a telephone that has a display panel and Soft Keys.

Supervisory Monitoring Announcement Tones

Before you use Supervisory Monitoring, make sure you are familiar with the announcement tone scheme. The system uses the announcement tones to indicate the status of Supervisory Monitoring to call participants.

- When the supervisor invokes either **Monitor** or **Whisper** mode, the agent might hear a tone, depending on how you configured the Supervisory Monitoring domain to which that agent belongs.
- When the supervisor invokes **Barge-In** mode, the agent and the external party might hear a tone, depending on how you configured the Supervisory Monitoring domain to which that agent belongs.
- When the supervisor invokes **Monitor** mode, a tone plays when the system prompts the supervisor to enter the agent's extension. You cannot disable this tone.
- Each of the three modes (**Monitor**, **Whisper**, and **Barge-In**) has a unique announcement tone.
- The tone accompanying the prompt for the agent's extension has the same pitch as the announcement tone.

Default Tones

Table 15 lists the default settings for Supervisory Monitoring.

Table 15 Supervisory Monitoring Announcement Tone Settings (Default)

Mode	Default Setting
Monitor	Off
Whisper	Off
Barge-In	On

Using Monitor Mode

The supervisor can use Feature Code **425** to invoke **Monitor** mode to monitor a conversation in progress. You can map this feature code to a button with or without a status light for individuals or groups. (Telephone users may change the button mapping for their own extensions only.)

1 Make sure that:

- You have enabled Supervisory Monitoring.
- You create a Supervisory Monitoring domain.
- You know the Supervisory Monitoring domain password. A telephone user who acts as the supervisor must know the Supervisory Monitoring domain password.
- The agent whom you want to monitor is a member of the Supervisory Monitoring domain.

2 On the telephone, press the programmable access button mapped to Monitor, or press the Feature button and use the keypad to enter Feature Code **425** for Monitor.

The system prompts for the domain password.

3 Enter the Supervisory Monitoring Domain password, then press either the *OK* menu option or # key, as appropriate.

- If the password or the extension is *invalid*, the display panel displays an error message and allows you to reenter the password.
- If the extension number is *valid*, the system plays a tone and prompts for an agent extension.

4 Enter the extension of an agent who is a member of the Supervisory Monitoring domain.

The system checks the state of the call that you are attempting to join and uses the display panel to inform you about the call status:

- If the agent is not on an call, the display panel displays *IDLE* and allows you to enter another extension.
- If the agent is not logged into the system, the display panel displays a message to that effect, and allows you to take another action.
- If the agent is already being monitored, the display panel displays a message to that effect, and allows you to take another action.
- If the agent is free to be monitored, the conversation becomes audible, and the system plays an announcement tone if it has been configured to do so.

  While you monitor a call, you can change the agent extension and the supervisory monitoring mode.

5 To end the Monitor session, hang up the telephone receiver.

The supervisor's display panel is the only display panel that displays menu options or indications that the Supervisory Monitoring feature is in use. (The agent's display panel does indicate that Supervisory Monitoring is in use.)

Changing Agents and Changing Modes While Monitoring

While you listen to a call in **Monitor** mode, the telephone display panel provides options to allow you to choose **Barge-In** mode, **Whisper** mode, or to change to another agent's call.

The display panel displays the extension of the agent currently being monitored, as well as these menu options:

- **Whisp**
- **Chg**
- **BrgIn**

Entering Whisper Mode From Monitor Mode While in **Monitor** mode, the supervisor can invoke **Whisper** mode.

The supervisor in **Whisper** mode can join, as well as listen to, the conversation between the agent and the customer. For example, the supervisor can provide information or a suggestion to the agent. The agent hears the supervisor's suggestions in addition to the conversation with the customer. The customer can hear the agent only.

*To enter **Whisper** or **Barge-In** mode, you must first enter **Monitor** mode, then switch to the appropriate mode.*

1. Press the **Whisp** Soft Key on your telephone.

   The agent might hear an announcement tone depending on how you configured Supervisory Monitoring.

2. Hang up the telephone receiver to end the Monitor session.

Entering Barge-In Mode From Monitor Mode While in **Monitor** mode, the supervisor can invoke **Barge-In** mode.

Barge-In mode immediately inserts the supervisor into the conversation with the agent and the customer. The supervisor, agent, and customer can hear and speak with the other parties in the conversation.

*To enter **Whisper** or **Barge-In** mode, you must first enter **Monitor** mode, then switch to the appropriate mode.*

1. Press the **BrgIn** Soft Key on your telephone.

   The agent might hear an announcement tone, depending on the way you configured Supervisory Monitoring.

2. Hang up the receiver to end the Monitor session.

Changing Agents While Monitoring a Conversation While in **Monitor** mode, the supervisor can change which agent to monitor.

1. Press the **Chg** Soft Key on your telephone.

   The system prompts for the agent extension and plays a tone.

2. Enter the new extension and press the *OK* menu option or **#** key, as appropriate.

   The previous agent's call is no longer audible to you and the current agent's call becomes audible. The current agent might hear an announcement tone, depending on the way you configured Supervisory Monitoring.

3. Hang up the receiver to end the Monitor session.

Supervisory Monitoring Usage Notes

This section describes general information about Supervisory Monitoring. Topics include:

- Special Considerations

- Supervisory Monitoring Error Conditions

Special Considerations

To configure Supervisory Monitoring, you must have Administrator access rights to the system. If you are a call supervisor, make sure you are familiar with the following issues when monitoring calls in progress:

- You can monitor calls internal to the system or external calls.
- You can monitor a call across a Virtual Tie Line (VTL).
- Any one of the parties involved in a Supervisory Monitoring environment (customer, agent, or supervisor) can put the call on hold and answer another call.
- You cannot invoke session-modifying services during a call being monitored. You can invoke the following telephone features during a call:
  - Forward voice mail
  - Do Not Disturb
  - Mute
  - Hold

  The display panel displays the message `Not allowed` if you invoke any other features during a monitoring session.
- If the customer or the agent invokes a session-modifying service such as Transfer, Conference, Call Park, or Transfer to Voice Mail, the system drops the supervisor from the call.
- You can use third-party TAPI applications to monitor calls.
- You cannot monitor more than two calls at the same time. Of the two calls, only one can be active at any given time; the other call must be on hold.
- You can monitor other supervisors. However, you cannot monitor a supervisor who is monitoring another call.
- Multiple supervisors can monitor different calls by the same agent. However, a specific call can be monitored by one supervisor only at any one time.
- If you exit the monitoring session, the call between the customer and the agent is unaffected.

- You cannot invoke Supervisory Monitoring if the supervisor is already on an active call.
- When you invoke **Barge-in** and either the caller or the agent subsequently puts the call on hold, you are still able to talk to the remaining party.
- The telephone user does not need to be an agent to be in a monitored call, nor does this user have to be logged in.
- An agent in a monitored call can transfer a call to another party.
- A primary telephone configured with bridged extensions could receive a call that an associated secondary telephone, which is not a part of a hunt group, ACD, or route point, can answer.

Restrictions in Monitoring ACD Calls There are a few cases in which you cannot monitor an ACD call, though the system is processing the call as an ACD call.

- You cannot monitor ACD calls going through call coverage to voice mail or Auto Attendant.
- Multiple supervisors cannot monitor the same agent at the same time.

  Supervisory Monitoring is limited to one active supervising session per agent.

Supervisory Monitoring Error Conditions

This section describes the most common Supervisory Monitoring errors and the results that occur. If appropriate, the table lists corrective measures that you might take to recover from errors.

- Feature Interaction Errors
- Validation Errors
- Supervisory Monitoring Service Errors
- Device Errors

Table 16 Feature Interaction Errors

Event	Action
A feature is active on the supervisor's phone that prevents Supervisory Monitoring.	The display panel displays an explanatory error message and the phone returns to the Ready state.

Table 16 Feature Interaction Errors

Event	Action
The agent or the customer hangs up while the supervisor has the call on hold.	The display panel cannot display messages while a call is on hold; the supervisor's phone immediately returns to the Ready state.
Supervisory Monitoring fails to start because two Supervisory Monitoring services are already active on the supervisor's device.	The display panel displays an explanatory error message and the phone immediately returns to the Ready state.
The agent or the customer invoke a feature that cannot operate with Supervisory Monitoring while the supervisor is monitoring the call.	The display panel displays an explanatory error message and the system gives the supervisor the option to change agents.
A feature is active on the agent's telephone that prevents Supervisory Monitoring from starting.	The display panel displays an explanatory error message and the system gives the supervisor the option to change agents.
An agent puts an ACD call on hold before the supervisor invokes Supervisory Monitoring.	The display panel displays an explanatory error message and the system gives the supervisor the option to change agents.

Table 17 Validation Errors

Action	Result
The supervisor enters an incorrect password or extension.	The display panel displays an explanatory error message and the system gives the supervisor the options to try again or exit.
The supervisor enters an incorrect password three times.	The display panel displays an explanatory error message and the phone exits Supervisory Monitoring and returns to the Ready state.
The supervisor enters the extension of a device that cannot be monitored (for example, the extension is a paging, Call Park, or Voice Mail extension).	The display panel displays an explanatory error message for five seconds, and then the system prompts again for the extension of an agent.

Table 18 Supervisory Monitoring Service Errors

Action	Result
Another supervisor is already monitoring the call.	The display panel displays an explanatory error message for five seconds, then the system prompts again for the extension of an agent.
The agent is not on any call.	The display panel displays an explanatory error message for five seconds, then the system prompts again for the extension of an agent.
The agent hangs up before the monitoring message reaches him causing Supervisory Monitoring to timeout.	The display panel displays an explanatory error message for five seconds, then the system prompts again for the extension of an agent.

Table 19 Device Errors

Action	Result
The supervisor's device does not support conferencing.	The display panel displays an explanatory error message and the phone returns to the Ready state.
The monitored agent's device does not support conferencing.	The display panel displays an explanatory error message and the system prompts again for the extension of an agent.
The customer's device does not support conferencing.	The display panel displays an explanatory error message and the system gives the supervisor the option to change agents.

Speed Dials

You can create up to 100 System Speed Dial numbers. You can also create system speed dial and personal speed dial button definitions and assign them to groups.

Do not confuse use speed dial codes with extension numbers.

Any telephone in a Telephone Group has access to the same button definitions. Telephone users can create personal speed dial definitions for buttons that do not already have a button mapping. Telephone users can also change definitions for any buttons mapped as personal speed dial buttons, even if those buttons are defined in the Group Button Mappings.

System speed dial numbers are not subject to Class of Service (CoS) restrictions. Therefore, a speed dial number mapped to a number that is a toll call is available to telephone users even if their CoS does not allow toll calls. Personal speed dial numbers are subject to CoS.

To set up system speed dials:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *Feature Settings* > *System Speed Dials*.
3. See the online Help for information about how to configure system speed dials.

WhisperPage

The WhisperPage feature allows you to dial an extension that is involved in an active conversation with another person and speak to that person without the other party on the call being able to hear you.

WhisperPage is typically used in the workplace by an assistant and manager. While a manager is on a call, an assistant can start a WhisperPage session to alert the manager of an important meeting or call. During the WhisperPage session, the assistant cannot hear the manager or the third party speaking and the third party cannot hear the comments of the assistant.

If the manager is not on an active call when the assistant starts a WhisperPage session, the system places the call as if the assistant dialed the manager's extension.

A typical WhisperPage session occurs as follows:

1. An assistant initiates a WhisperPage through Feature Code **426** or a programmed system access button, depending on the type of telephone and how it is configured.
2. The manager might hear an alert tone announcing the WhisperPage request.

   The display panel on the manager's phone shows the Caller ID of the assistant and the WhisperPage icon for 5 seconds, and then the display reverts back to the Caller ID information of the person the manager is speaking with.

The manager also has a period of time, called the Decline Time, to refuse the WhisperPage. You can configure WhisperPage behavior by enabling or disabling the alert tone and specifying the Decline Time to be 0 – 9.9 seconds in 0.1 second intervals. The default Decline Time is two seconds.

You can also configure, on a per-user basis, the WhisperPage feature success tone waiting time period that the assistant hears.

3 To accept the WhisperPage, the manager does nothing.

When the Decline Time period expires, the assistant hears a tone that indicates that the WhisperPage session is active. The display panel on the assistant's phone displays `Whispering` and the manager's extension to indicate that the WhisperPage session is active. The assistant can speak to the manager. The other party on the call does not hear the assistant's comments and the assistant cannot hear the manager or the person to whom the manager is speaking.

4 To refuse the WhisperPage, the manager can invoke the Do Not Disturb (DND) feature during the Decline Time.

The assistant hears an error tone and the display panel on the assistant's phone shows a message that indicates that the WhisperPage was unsuccessful. The manager can also invoke DND to end an active WhisperPage session. If the manager invokes DND, the feature is active until the manager disables it.

5 The assistant hangs up to end the WhisperPage session.

You can configure the WhisperPage announcement tone that the manager hears on a per-user basis:

1 Click *Feature Settings* > *WhisperPage.*

2 Click a domain and then click the extension of a member of that domain

The system displays the Report window.

3 Type a value in the *Decline Time* field.

4 Click *OK*.

However, you cannot configure the WhisperPage feature success tone heard that the assistant hears.

You may can Feature Code **426** for WhisperPage to a telephone button for individuals or groups. Telephone users may change the button mapping for their extension only if you have extended this privilege using

the CoS function. You can configure the mapped buttons from the Button Mapping window. Click *Telephone Configuration* > *Telephones* or *Telephone Configuration* > *Telephone Groups*. Click a telephone extension or a telephone group name, depending on which sub menu you chose, and then click the Button Mapping tab.

WhisperPage Permissions

Both the manager and the assistant in a WhisperPage session must be assigned to a WhisperPage domain and have appropriate WhisperPage access privileges.

Telephone users can view their WhisperPage access privileges from within the NBX NetSet utility. WhisperPage permissions include this information:

- Whether or not the WhisperPage alert tone is enabled
- The waiting time before an initiated WhisperPage session becomes active
- Telephone users (listeners) to whom you can initiate a WhisperPage session
- Telephone users (speakers) who can initiate a WhisperPage session with you

You can define these access privileges when you create the WhisperPage domains.

Using Domains For WhisperPage

A *domain* is a grouping of telephone users who are logically associated in some way. You create domains for use with the WhisperPage feature.

Each domain must have a unique name, which you configure in the NBX NetSet utility (click *Feature Settings* > *WhisperPage*).

For each domain in the system, configure the following:

- The list of members in that domain to whom speakers can whisper.
- A list of members in that domain who can invoke the WhisperPage feature.

You can create a domain with no members. There can be a maximum of 50 domains in the system. (Some platforms might support fewer domains due to resource usage.)

The Report window shows the extensions to which a telephone user can whisper, and also shows the extensions that are able to whisper to the telephone user.

1. Click *Feature Settings* > *WhisperPage*.
2. Click a domain.
3. Click the extension of a member of that domain to display the Report window.

Feature Interaction With Whisper Page

This section describes how the WhisperPage feature interacts with other system features.

Feature	Manager	Assistant
Account Code	Allow	Disallow
CO Flash	Allow	Disallow
Conference	Allow - drop assistant	Disallow
Conference drop	Allow	Disallow
COS Override	Allow	Disallow
Directory	Allow	Disallow
Direct Mail Transfer	Allow - drop assistant	Disallow

Feature	Manager	Assistant
Fwd RNA	n/a	Disallow
Fwd Busy	n/a	Disallow
Fwd DND	Allow - drop assistant	Allow
Handsfree	Allow	Allow
Hold	Allow - drop assistant	Allow (no Music On Hold)
Mute	Allow	Allow
Speakerphone	Allow	Allow

Feature	Manager	Assistant
Call pickup	n/a	n/a
Speed dial	Allow (ignore)	Disallow
Line redirect	n/a	Disallow
Toggle Fwd to VM	Allow	Allow
Release	Allow - drop assistant	Allow

Feature	Manager	Assistant
User park	Allow - drop assistant	Disallow

Feature	Manager	Assistant
Hunt Group Logging	Allow	Disallow
Hunting Service	n/a	n/a
Last Number Redial	Allow	Disallow
Lock unlock	Allow	Disallow
Orig startup	n/a	n/a

Feature	Manager	Assistant
System info	Allow	Disallow
Term startup	n/a	n/a
Transfer	Allow - drop assistant	Disallow
User password	Allow	Disallow
Camp On	Allow - drop assistant	Disallow
Volume Up / Down	Allow	Allow

Feature	Manager	Assistant
VTL merge	n/a	n/a
Bridged phones	Allow	n/a
Mapped TLIMs	Allow	n/a
VTLs	Cannot go across VTL	Cannot go across VTL

WhisperPage Restrictions

WhisperPage restrictions include:

- Only the administrator can:
  - Create a domain
  - Add telephone users to a domain that allows WhisperPage to be invoked
  - Add telephone users to a domain that allows a WhisperPage to be received on a particular extension
- Multiple assistants cannot whisper to the same extension at the same time.

- An assistant may initiate only *two* WhisperPage sessions at any one time (one or both on hold), provided that there is a line available for each session.
- While using WhisperPage, if the party speaking to the manager hangs up and terminates the call, the system disconnects the assistant from the call.

  The system displays an error message to the assistant on the display panel and plays a feature error tone.
- The assistant and the manager must be on the same system.

  You cannot use the WhisperPage feature over VTL /Q.SIG/ T1 tie lines or /PRI / BRI/ T1 E&M robbed bit lines.
- The system has a resource pool of 42 multicast addresses for the WhisperPage feature.

  There are no limits as to the maximum number of multicast addresses that any one feature can use. It is possible for another feature to exhaust the addresses in the resource pool.
- Use the DND feature to implement Decline Whisper.
- On an ATA, any feature that the manager tries to invoke disconnects the assistant from the call.

  If the manager presses flash hook on an ATA to enter a feature code, the system invokes hold on the manager's device.
- On an ATA, a telephone user cannot distinguish the difference between Supervisory Monitoring Whisper Mode and WhisperPage.

  There is no display panel on an ATA, and the tone is identical for both features.

For more information about configuring WhisperPage, see the online Help.

4 System Maintenance

This chapter describes how to manage system-level maintenance operations for the system, including:

- System Backup
- System Restore
- Import / Export Data
- Reboot/Shutdown
- Password Administration
- Call Report Settings
- Purge Database
- Disk Mirroring

For more information about these topics and configuration procedures, see the online Help.

System Backup

You can back up a system database at any time. To ensure a successful restoration of your database, be sure that the version number of the backup file matches the version number of the system software.

For example, to restore the data on a system running release R6.0, use a backup file from release R6.0, not from release R5.1 or lower. If you restore a database that you saved on an older release, the operation will succeed. However, if there is a change in the database schema between the old and new releases, the restore will fail.

CAUTION: *3Com does not support the restoration of a database from an older version of the system software.*

3Com recommends this backup policy:

- Back up your database before you upgrade the system software.

- When you upgrade system software, answer *Yes* when the software prompts you to include the database in the upgrade process.
- After an upgrade, backup the database again.
- After you make any administrator-level configuration changes, backup the database.
- To ensure that you capture changes that telephone users make to their personal settings, perform frequent or, if possible, daily backups.

A backup of your system data includes voice mail messages and licenses only if you specify that you want to include them. If voice mail was not included when the system data was backed up, you cannot specify that you want to restore voice mail during a restore operation.

During a backup operation, a series of status windows track the steps. Some steps might occur quickly so that you do not see the status window. For example, you might see the status window appear to go from step 1 to step 4, if steps 2 and 3 complete quickly.

A system task, which is independent of all other system tasks, backs up your database. You can safely perform any of these actions before the backup operation completes without interfering with the backup:

- *Click your browser's* Back *button*
- *Click your browser's* Stop *button*
- *Exit your browser*
- *Shut off your computer*

If another administrator tries to back up the system database before the current backup task completes, a message warns that a backup is currently in progress.

The message includes:

- The IP address of the computer from which the backup was started
- The time that the backup was started
- The current step of the upgrade process

The seven steps in the backup operation include:

1. **Backup Starting** — The system begins the backup operation. The status window displays step 1 of 7.
2. **Backing up Database** — The system locks the databases during this step. The status window displays step 2 of 7.
3. **Backing up Voice Mail** — If you enable the Include NBX Voice Mail check box, the system backs up voice mail messages for all telephone users. The system locks Auto Discovery and voice mail access during this step. The status bar displays step 3 of 7.
4. **Backing up Voice Mail Data** — The system backs up greetings and name announcements of all telephone users. The status bar displays step 4 of 7.
5. **Backing up License** — The system backs up licenses on the system. The status bar displays step 5 of 7.
6. **Creating Backup file** — The system adds all files created during the backup process to a single backup file. The status bar displays step 6 of 7.
7. **Backup Finishing** — The system deletes temporary files created during the backup operation. The status bar displays step 7 of 7.

Saving the Backup File

After the system completes the backup operation, the final window displays the name of the backup file and gives you the opportunity to save the file in a location you choose, which is typically on the disk drive of your PC or on the disk of another computer in your network. 3Com recommends that you save the backup file when prompted to do so.

The system keeps a copy of the most recent backup file on your system. Each time you perform a backup operation on the database, the system overwrites this file.

If you choose to not save the backup file during the backup procedure or if you forget to save it, you can save it later. However, if you perform another backup, the prior backup file is no longer available.

Cancelling a Backup Operation

You can cancel the currently active backup operation. When you click *Cancel*, the system immediately asks you to confirm that you want to cancel the backup operation. If you click *Yes*, the system first completes

the current step of the backup operation and then cancels the backup operation.

Depending on the size of your database, some of the steps in the backup operation can take several minutes to complete. Please allow time for the system to complete the current step and respond to your cancel command.

System Restore

You can restore a database using a backup file that is from the same version as the running system software. For example, to restore the data on a system running version R4.3.3, use a backup file from R4.3.3; do not use a backup file from R4.3.2 or lower. If you restore a database that you saved on an older release, the operation will succeed. However, if there is a change in the database schema between the old and new releases, the restore will fail.

You can convert configuration data stored with an older software version to a newer software version. You might need to do this if you have installed a new version of the software but you want to use older configuration data. During normal operation, you do not need to use this function.

CAUTION: *3Com does not support the restoration of a database from an older version of the system software. In addition, you can severely damage an NBX 100 system if you try to restore a database from a V5000,V3000, or V3001R system. Do not attempt this operation under any circumstances.*

The backup of your system data includes voice mail messages only if you specify that you want it included. If voice mail was not included when the system data was backed up, you cannot specify that you want to restore voice mail during a restore operation.

Backing up and restoring your licenses are procedures that are separate from the database backup and restore procedures. Back up your licenses before and after you add or remove any licenses.

To restore your database from a saved backup file:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *System Maintenance > System Restore.*

3. Browse to locate the current backup file or use the drop-down list to select an earlier software version from which to convert configuration data.
4. Click *Restore Database.*

   The system provides cautionary information about the effect of a restoration on system operation and prompts you to confirm that you want to restore the database.
5. Click *Yes* to restore the database.

   The system automatically reboots after the database file is loaded.

Import / Export Data

You can to import telephone data from a file on a PC to the database, or export telephone data from the database to a file on a PC (click *System Maintenance > Import/Export Data*).

The data is in .CSV format, which is a Microsoft Excel convention. This method lets you populate many telephone user records into the database in a single operation.

CAUTION: *Make sure you are familiar with data in this format before you import or export data. Otherwise, you might inadvertently propagate incorrect data into the database.*

Each record of the data consists of the following fields:

- Extension
- First(Name)
- Last(Name)
- Title
- CoS
- Location1
- Location2
- Department
- Telephone Group
- Device Type
- MAC Address

- Channel
- Forward to Auto Attendant
- Receive Maintenance Alert
- Exclude from LCD
- Exclude from Name Directory

To manage these settings, click *Telephones* and *System-Wide Settings.*

Reboot/Shutdown

You must reboot the system after you upgrade software and you must shut down the system software before you turn off power to your system.

To reboot or shutdown the system:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *System Maintenance* > *Reboot/Shutdown*.
3. See the online Help for procedures to reboot and shut down the system.

CAUTION: *If you remove power from the system without first shutting down the system software using the NBX NetSet Shutdown function, the operating system must perform a file system check during the next startup cycle to ensure file integrity. The file system check significantly increases the time it takes for the system to come to a ready state. During a file system check operation, the Call Processor's S1 and S2 status lights flash in an alternating pattern.*

Password Administration

The Password Administration window enables you to manage passwords. The most common use is to reset a telephone user's forgotten password.

To set system passwords:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *System Maintenance* > *Password Administration*.
3. From the drop-down list, select which of these types of passwords you want to set:

- **Change Administrator Password** — Resets the password for administrator access to NetSet.

  After you change an administrator password, make sure you record the new password appropriately. There is no "back door" password to use if you lose this password. If you change the default 4-digit password to an 8-digit or longer password, you cannot revert to a 4-digit password.

- **Reset User Password** — Resets the password to a telephone user's extension. After you reset the password, instruct the telephone user to change to a new password as soon as possible to ensure system security.

- **Auto Attendant Password** — Limits access to Auto Attendant settings and functions.

- **System Backup Password** — Enables automated backups from an external system.

- **General Call Data Reporting Password** — Limits access to Call Detail Reports, an optional component of the system. See "Call Report Settings" on page 82 for more information.

- **ACD Call Data Reporting Password** — Limits access to ACD Call Detail Reports.

- **Virtual Tie Lines Password** — Enables calls over Virtual Tie Lines (VTLs) to "hop off" after they reach the destination system. The call then appears to originate at the destination system. See Chapter 11 for more information about setting up VTLs.

- **Hunt Group Voice Mail Password**— Resets the password for the Hunt Group extension number.

- **Hunt Group Supervisory Monitoring Password**— Resets the password that allows the Hunt Group supervisor to monitor calls to hunt group members.

- **ACD Group Voice Mail Password**— Resets the password for the ACD Group extension number.

- **ACD Group Supervisory Monitoring Password**— Resets the password that allows the ACD Group supervisor to monitor calls to ACD group agents.

- **TAPI Voice Mail Password**— Resets the password for the TAPI Route Point extension number.

- **TAPI Route Point Supervisory Monitoring Password**— Resets the password for the Hunt Group supervisor to monitor calls to hunt group members.

Call Report Settings

The Call Processor captures information about all outgoing and incoming calls made through the system. To view this call information in detail, install Call Reports (*Downloads > Applications > NBX Call Reports*) on a networked computer as specified later in this section. Then, download the call report information, which is referred to as call detail reports, from the system to a local hard drive.

After you install the NBX Call Reports software, you can:

- Retrieve calling data from the system.
- Generate formatted reports.
- Export reports in formats suitable for use with third-party reporting software, spreadsheets, databases, and word processing applications.
- Export your call data in HTML format for publication on a web server.
- Export reports to a disk file or directly to a Microsoft mail message or a Microsoft Exchange folder.

CDR Changes At Release R6.0

The release R6.0 system software has enhanced NBX Call Reports to provide more data clarity and completeness for the CDR client reports.

These CDR enhancements include the following:

- Logs the call records in XML format.
- Logs all parties in the call.
- Logs a record each time the call topology changes (that is, whenever another party is added or removed).
- Logs feature data on a per-party basis (that is, one or more sets of feature data can be present in the same CDR record).
- Logs external as well as internal calls. If you want to view external calls only, you can select the external call report.
- Supports backward compatibility for R5.0 CDR clients.
- Introduces new data fields as subtags wherever necessary.

Additional CDR Fields

There are five new CDR fields at release R6.0. Two fields pertain to all basic calls in release R6.0.

- **Call Answered Time** — A timestamp that indicates when the call was answered. (This is a mandatory field.)
- **CallPrivacy** — Enables calls marked as Private to be treated as private calls. (This is an optional field.)

The other three new fields are subtags, each of which are associated with a feature.

<Facd> — This subtag appears only for those parties having ACD data. This is placed under the **party** tag. (This is an optional tag.)

<Fmwb> — This subtag appears only for those parties having Supervisory Monitoring data. This is placed under the **party** tag. (This is an optional tag.)

<Fwp> — This subtag appears only for those parties having WhisperPage data. This is placed under the **party** tag. (This is an optional tag.) **<Fwp>** uses the some of the fields that are present under the **<Fmwb>** subtag.

New File Format

Release R6.0 requires CDR to use XML instead of CSV as a file format. However, the NBX NetSet utility allows you to choose the file format you wish to use.

The use of the XML format will be enforced at a future release.

Use the following table to understand the relationship between CRD at previous releases and release R6.0:

Current CDR Installation	Configuration	Description
CDR 6.0 (NBX)	Select the option **Enabled for XML**	All CDR records are in XML format, including the CDR records for the release R6.0 feature.s

Current CDR Installation	Configuration	Description
CDR 5.0 (NBX)	Select the option **Backward Compatible for CSV**	The records are in CSV format; this does not include any new records for release R6.0 features. This is the default option when customers upgrade from release R5.0 to release R6.0. All settings related to purge interval and logging of internal calls are retained as in release R5.0.
pre-R5.0 CDR (NBX)	There is no option for supporting pre-R5.0 CDR operations. Select the option **Enabled for XML**.	If clients upgrade from pre-release R5.0 versions to the CDR 6.0 version directly, then backward compatibility is not provided, and clients must view the CDR records in XML format. If clients must view CDR records in CSV format, the upgrade path is as follows: pre-R5.0 CDR > CDR 5.0 > CDR 6.0
CDR Client 6.0	Interaction with release R5.0	Unsupported
CDR Client 6.0	Interaction with release R6.0	Supported
CDR Client 6.0 and CDR Client 5.0	Installation on same device	Unsupported. You cannot install the release R6.0 and release R5.0 clients on the same device.

Call reports do not include information about the locked or unlocked status of telephones.

Windows Environment Specifications

Your computer must meet these minimum requirements to run Call Reports:

- **Processor** — Pentium 166MHz or higher
- **Operating System** — Windows 2000 (Service Pack 2) or Windows XP
- **RAM** — 64 MB on Windows 2000; 128 MB on Windows XP
- **Network** — Network connectivity to the Call Processor
- **Disk Space** — At least 40 MB of free disk space

Installing Call Reports

To install NBX Call Reports:

1. Click *Downloads* > *Applications*.
2. Enable the *NBX Call Reports* radio button.
3. See the online Help topic for information about installation procedures.

Configuring Call Reporting

You can configure your system to save call information, and then use the Call Reports function to view the information in a variety of formats. You can create a password-protected logon for telephone users so that the users can access call report information. This logon does not provide administrator privileges to telephone users.

Call Detail Report (CDR) records incorporate caller ID information to identify a caller. VTLs transmit a maximum of 30 characters for the caller ID, which might cause longer caller IDs to lose excess characters. See "Creating a Pretranslator for VTL Calls" on page 297 for more information about how to configure a VTL pretranslator to avoid inaccurate data in CDR records.

To configure call reporting, click *System Maintenance* > *Call Report Settings* and see the online Help for more information.

The software supplied by or on behalf of 3Com has the ability to mask or scramble the last four digits on call records. If you do not select this function, the software records call numbers without any digits masked or scrambled.

The collection, storage, or manipulation of personal data such as these call numbers might incur obligations under local laws, such as those relating to data protection or privacy. These legal requirements differ from country to country and it is your responsibility to comply with all such obligations.

3Com accepts no liability for your failure to comply with local laws regarding the collection, storage, or manipulation of such information and data.

Purge CDR

You can purge old Call Detail Report (CDR) data from the system.

To purge CDR data:

1. Click *System Maintenance* > *Call Report Settings*.
2. Click *Purge CDR*.

Purge Database

When you purge the database, the software removes existing telephone user and device data that you added to the system, restores factory defaults, and causes an automatic reboot.

To purge data:

1. Click *System Maintenance* > *Purge Data*.
2. Click *Purge Database*.

The Purge Database feature does not affect your IP connectivity to the NBX NetSet utility. After a database purge, the system continues to use the IP address, subnet mask, default gateway, and host name that you have assigned.

Purge Database and CDR

You can purge Call Detail Reports (CDR) data at the same time that you purge telephone user and device data.

To purge data and CDR data:

1. Click *System Maintenance* > *Purge Data*.
2. Click *Purge Database and CDR*.

You might need to purge your existing CDR records if you perform an upgrade. See the appropriate Software Upgrade Guide *for details.*

Purge All Voice Mail

You can delete all voice mail messages for all telephone users.

To purge voice mail:

1. Click *System Maintenance* > *Purge Data*.
2. Click *Purge all Voice Mail*.

Mailbox greetings are not affected.

Manage Data

This section describes these system data management operations:

- Migration
- Restore Database From Another Version

Migration

Table 20 describes the supported migration paths to move your data from one system platform to another.

Table 20 Data Migration Platforms and Software Revisions

Source	Target*	Notes
NBX 100	V5000	The NBX 100 must be at release R4.2.X or higher.
	V3000	
V3000	V5000	The V3000 system must be at release R4.4.X or higher.
	NBX 100	Unsupported.
V5000	V3000	The V5000 system must be at release R4.2.X or higher.
	NBX 100	Unsupported.

* Must be release R5.0 or higher.

Data Migration Notes and Prerequisites

Before you begin a data migration, make sure you understand these important prerequisites:

- You cannot simply remove the disk drive from one type of system platform and install it into a different platform. If you attempt to do so, the system will not boot properly.
- Licenses are not part of a database migration. The licenses on your old system will not work on the new system. Your new system comes with its own set of license keys that you must enter into the new system before you migrate your data.
- The target system must be licensed to support the capacities of the source system. For example, you cannot move the data from a V5000 system with 1000 devices successfully onto a V3000 system, unless you install the memory upgrade and a license to support at least 1000 devices on the V3000 system.
- You can choose to include or exclude telephone users' voice mail messages when you perform the data migration.
- The system software version on the target system must be equal to or higher than the software version on the source system. For example, you cannot move data from a release R5.0 system onto an release R4.3 system using the data migration feature. The target system software must be at release R5.0 or higher.

- A data migration operation does not alter data. For example, it will not change extensions. To change between a 3-digit dial plan and a 4-digit dial plan requires a separate series of steps, which "Converting Extensions" in Chapter 11 describes.

Migrating Data

To migrate data from one platform to another, use the NBX NetSet utility to perform a backup operation on the source platform and then perform a restore operation, using that backup file, on the target platform. Perform the migration outside of regular business hours so that the migration does not impact telephone users.

To migrate data:

1. Install the target system.
2. Install your license keys on the new system.

   Note that you need new license keys for the new system. You cannot load a license backup file from the old system nor can you use the license keys from the old system. License keys are generated from each system's unique system ID number.
3. Perform a backup operation on the old system (click *System Maintenance > System Backup)*.
4. Enable the *Include NBX Voice Mail* and *Include NBX Licenses* check boxes if you want telephone users' voice mail messages and licenses to be available on the new system.
5. Use the backup file you just created and perform a database Restore operation on the new system (click *System Maintenance > System Restore).*

Restore Database From Another Version

You can migrate configuration data stored with an older software version to a newer software version. You might need to do this if you install a new version of the software but you want to use older configuration data. During normal operation, you do not need to use this function.

From the System Restore window (click *System Maintenance > System Restore*), select the source version from which you want to migrate the data and click *Restore Database*.

Disk Mirroring

The V3001R and V5000 systems supports disk mirroring, using RAID1 technology, to provide data security and throughput speed. When you fully partner the mirror disk with the master system disk, the system writes all data to the mirror disk as well as to the master disk. If data is read from disk, the software can read from either disk, which can improve data access times.

If either disk fails in a fully mirrored system, the system software uses only the remaining good disk, and system operation continues. Status information is available on the Call Processor front panel status lights to indicate when a disk fails and which disk to replace. After you replace a failed disk and restart the system, the software brings the new disk up to a fully mirrored state. The system typically takes from 30 to 90 minutes to complete the mirroring process, depending on the amount of data on the master disk.

Adding a Mirror Disk

If your V3001R or V5000 system uses a single disk, you can add a mirror disk. The disk you add must have at least the same storage capacity as the disk in the system. You must obtain a disk mirroring license to convert a single-disk system to use disk mirroring. You also need a Phillips screwdriver to complete this process.

CAUTION: *When you add a mirror disk, you must perform a system database backup and a system shutdown. 3Com advises that you add a mirror disk during nonbusiness hours.*

To add a mirror disk:

1. Back up the database on the system:
   - **a** Click *System Maintenance* > *System Backup* > *Backup.*
   - **b** Specify a location for the backup file.
2. Install the disk mirroring license:
   - **a** Obtain the license key from your dealer.
   - **b** Click *Licensing and Upgrades* > *Licenses* > *Add License.*
   - **c** Type the license key in the License Key field.
   - **d** Click *OK*.
3. Shut down the system (click *System Maintenance* > *Reboot/Shutdown* > *Shutdown*).

4 Install the second disk drive:

   a Unlock the disk tray.

   b Unscrew the two retaining screws.

   c Remove the disk tray.

   d Connect the IDE disk cable to the disk drive.

   e Connect the power harness to the disk drive.

   f Fasten the new disk to the disk tray using your Phillips screwdriver and the screws provided with the disk.

   g Reinsert the disk tray.

   h Screw in the two retaining screws and lock the disk tray in place.

5 Restart the system.

6 Verify that the disks begin the mirroring process.

   On the Call Processor front panel, check the four status lights under the PWR and S1 labels. The status lights labeled 1, 2, and 3 (Figure 3) indicate disk status.

Figure 3 Disk and Power Status Lights

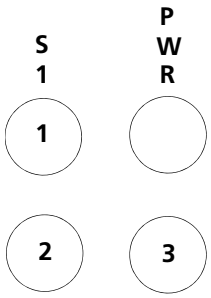


Table 21 describes the possible states of the status lights.

Table 21 Disk Status Light States

Explanation	LED 1	LED 2	LED 3	PWR
Attempting to boot from disk 0 (zero)	Off	On	Off	On
Attempting to boot from disk 1	Off	Off	On	On
Boot process complete, system initializing	Flashing	N/A	N/A	On
System is running	On	N/A	N/A	On

Table 21 Disk Status Light States (continued)

Explanation	LED 1	LED 2	LED 3	PWR
Flash codes indicate disk problem: ■ **2 flashes**: No valid disk (system is halted) ■ **3 flashes**: Two valid disks, but they are not paired (system is halted) ■ **4 flashes**: Configuration problem (system is halted) ■ **5 flashes**: Two disks present, but no mirroring license	N/A	Flashing	Flashing	On
Using disk 0 (zero) only	N/A	On	Off	On
Using disk 1 only	N/A	Off	On	On
Synchronizing — disk 0 is valid, disk 1 is becoming a fully mirrored disk. LED 3 flash rate indicates progress. If LED 3 stops normal flashing and intermittently flashes twice, the mirroring process has failed.	N/A	On	Flashing	On
Synchronizing — disk 1 is valid, disk 0 is becoming a fully mirrored disk. LED 2 flash rate indicates progress. If LED 2 stops normal flashing and intermittently flashes twice, the mirroring process has failed.	N/A	Flashing	On	On
LED 2 and LED 3 flash alternately: the two disks are resynchronizing	N/A	Flashing	Flashing	On
Synchronized	N/A	On	On	On

Verifying a Failed Disk Drive

If either disk fails while in a fully mirrored state, the system continues to operate. The disk status light states described in Table 21 indicate which drive has failed.

To verify the status of a disk drive, see the Disk Status window:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *Reports* > *System Data*
3. Click *Disk Status*.

Reverting to a Single-Disk System

If disk mirroring is currently active, you can convert the system to operate with a single disk. You need a Phillips screwdriver to complete this process.

To revert to a single-disk system:

1. Use Table 21 to determine which disk is the mirrored disk.
2. Shut down the system (click *System Maintenance* > *Reboot/Shutdown* > *Shutdown*).
3. Remove the mirrored disk drive:
   a. Unlock the disk tray.
   b. Unscrew the two retaining screws.
   c. Remove the disk tray.
   d. Disconnect the disk data cable from the mirrored disk drive.
   e. Disconnect the power harness from the mirrored disk drive.
   f. Unfasten the mirrored disk from the disk tray using the Phillips screwdriver and the screws provided with the disk.
   g. Reinsert the disk tray.
   h. Screw in the two retaining screws and lock the disk tray in place.
4. Restart the system.
5. Use the NBX NetSet utility to remove the disk mirroring license from the NBX NetSet utility:
   a. Click *Licensing and Upgrades* > *Licenses.*
   b. Click *Remove License.*
   c. From the *Select License to Remove* drop-down list, select *Disk Mirroring License*.
6. Click *OK*.

5 TELEPHONE CONFIGURATION

This chapter describes how to configure and manage devices on the system. It describes these topics:

- Adding, Removing, and Modifying Telephones
- Adding a Remote Telephone
- Creating and Managing Bridged Extensions
- Creating and Managing Telephone Groups
- Recording and Monitoring Telephone Calls
- Creating and Managing Button Mappings
- Changing Device IP Settings
- Configuring the Attendant Console
- Connecting and Managing Analog Devices

For more information about these topics and configuration procedures, see the online Help.

For information about installing the system hardware components, see the NBX Installation Guide.

Adding, Removing, and Modifying Telephones

This section describes how to add, remove, and modify telephones in the NBX NetSet utility. You can also review the status of each device and configure button mappings for 3Com telephones.

Adding a New Telephone

You can use two methods to configure a new telephone:

- **Auto Discovery method** — Auto Discovery is the simplest and most common method to add a new telephone. When you enable Auto Discovery and then connect a new 3Com Telephone to the LAN, the new telephone receives the next lowest available extension number

and a default set of properties. The telephone's display panel displays the extension.

- **Manual method** — You can use the NBX NetSet utility to disable Auto Discovery and configure telephones manually. However, if you have many telephones to configure, manual configuration can be a tedious and error-prone process.

For either method, you need to connect the telephone to the network. If you use Auto Discovery, enable the Auto Discover Telephones check box *before* you connect the telephone. If you add a telephone manually, you can connect the telephone before or after you use the NBX NetSet utility to add it.

Connecting the Telephone

Instructions for connecting the telephone to power and the network depend on your power source and the type of telephone. See Chapter 3 in the *NBX Installation Guide* or the telephone packing sheet for telephone connection information.

Adding a New Telephone Using Auto Discovery

Before you enable Auto Discovery, verify that a 3-digit or 4-digit dial plan is installed on the Call Processor and that you have specified a starting extension. See the NBX Installation Guide *for more information.*

To add a new telephone using Auto Discovery:

1. Click *System-Wide Settings* > *Auto Discovery*.
2. Optionally, clear all check boxes associated with autodiscovering devices.
3. Enable *Auto Discover Telephones*, and then click *Apply*.
4. Optionally, enable the *Auto Add Phones to Call Pickup Group 0* check box.

Regardless of whether you select this check box, you can change the call pickup group for any telephone later. See "Call Pickup" on page 51 for more information.

5. Click *OK*.

For each telephone that you want to autodiscover:

1. Remove the telephone from the packing box.
2. Connect the telephone to power and the network according to the instructions in the telephone packing sheet or the *NBX Installation Guide*.
3. Wait until an extension number displays in the telephone's display panel.

Devices that require a license, such as the 3102 Business Telephone, the 3101 and 3101SP Basic Telephones, and the 3105 Attendant Console, do not display an extension number until you add the license to the system. If you have not entered a license for a telephone, its display panel displays the device's MAC address and a rotating hyphen.

You can now disconnect the telephone and move it to its destination. The telephone retains its extension and button mappings.

Adding a Telephone Manually

To add a new telephone manually:

1. Click *Telephone Configuration* > *Telephones*.
2. Click *Add*.
3. Enter the appropriate values in the fields.

   See the online Help for more information.
4. Click *Apply* to configure this telephone.

   You can configure additional telephones, if necessary.
5. Click *OK*.

Modifying a Telephone

To modify a telephone:

1. Click *Telephone Configuration* > *Telephones*.
2. Click the extension of the telephone that you want to modify from the list.
3. In the Modify window, change the desired fields.

   See the online Help for more information about the dialog box fields.
4. Click *OK*.

Checking a Telephone's Status

To check the status of a telephone:

1. Click *Telephone Configuration* > *Telephones*.
2. Click the extension of the telephone for which you want a status report.
3. Click the *Status* tab.
4. View the device status and see the online Help for information about options.
5. Click *OK*.

Removing a Telephone

To remove a telephone from the system:

1. Click *Telephone Configuration* > *Telephones*.
2. Select the telephone, or telephones, that you want to delete and click *Remove Selected*. To select all telephones, enable the *Select* check box.
3. Click *OK* when the dialog box prompts you so that the system removes the selected telephone.
4. Click *User Configuration* > *Users.*
5. Select the extension, or extensions, that you want to delete and click *Remove Selected*. To select all telephones, enable the *Select* check box.
6. Click *OK* when the dialog box prompts you so that the system deletes the selected extension.

If you do not delete the telephone user, the extension of the removed telephone becomes a phantom mailbox.

Rebooting a Telephone

To reboot a telephone:

1. Click *Telephone Configuration* > *Telephones*.
2. Click the extension of the telephone that you want to reboot.
3. Click the *Status* tab.

CAUTION: *If the telephone has an active call, you will disconnect the call when you reboot the telephone.*

4. Click *Reset Device* and then click *OK*.

   You can also reboot a telephone by unplugging the power connector from the telephone and then plugging it in again.

Adding a Remote Telephone

The system software (release R4.2 and higher) supports Network Address Port Translation (NAPT, also called NAT overloading). NAPT allows you to put a 3Com Telephone behind a device that applies network address translation at a remote location, such as a home office, and connect to the Call Processor through an Internet connection. A typical configuration is to connect a cable or DSL modem to a small office or home office router that includes a firewall and Ethernet ports. You connect the 3Com Telephone directly to one of the Ethernet ports. Another option is use the pcXset soft telephone application instead of an 3Com Telephone.

Remote NAPT Telephone Configuration

This section summarizes the tasks you must complete to configure a 3Com Telephone for operation behind the NAPT device. Because the configuration interface on each device varies, detailed procedures for NAPT device configuration are beyond the scope of this document. For information about configuring the NAPT device, see the documentation for that device.

To add a broadband connected telephone behind a NAPT device:

1. Make sure the system is set up for IP operations, either Standard IP or IP On-the-Fly. If you are not using a VPN connection to establish access from your home system to the system network, the system must have a public IP address.
2. Use the NBX NetSet utility to enable *Auto Discover Telephones* (*System-Wide Settings* > *Auto Discovery*) and then connect the 3Com Telephone to the system.

   Autodiscovering the telephone while it is connected locally to the network allows the system to configure the telephone in the system database and assign an extension number. You can manually add the telephone to the system database instead of using the Auto Discover feature.
3. Move the telephone to its intended location. Connect it to power and then use the telephone Local User Interface (LUI) utility to program these settings:
   - Call Processor MAC address — Required only when the network has more than one Call Processor.
   - Telephone IP address — A private IP address matching the IP address scheme on the LAN side of the NAPT device but outside of the DHCP address range configured in the NAPT device. The telephone must

have a static IP address. For the pcXset application, this is the IP address of the computer.

- Call Processor IP address — The IP address of the Call Processor with which the telephone must communicate. If you are not connecting to the network through a VPN connection, the system must have a public IP address.
- Subnet Mask — The address mask in use on the LAN side of the NAPT device.
- Default Gateway — The IP address of the NAPT device on the LAN.

For details about how to use the LUI utility, see "Using the Telephone Local User Interface Utility" on page 413.

4 Configure the NAPT device.

Use the device's user interface to map UDP ports 2093-2096 to the 3Com telephone IP address. These UDP ports are registered ports for system operations. This mapping feature, known as virtual server, port mapping, port range forwarding, or rules, is required to allow traffic to pass to and from the 3Com Telephone.

Creating and Managing Bridged Extensions

Bridged extensions allow you to have the extension of a primary telephone appear on one or more secondary telephones. Most activities associated with the extension can be performed on both the primary telephone and any of the secondary telephones. However, you cannot use a bridged extension on a secondary telephone to place a call.

On any system, you can configure a maximum number of primary telephones and a maximum number of bridged extensions on primary telephones. See Table 22.

Table 22 Maximum Bridged Extensions

System	Device Limit	Maximum Number of Primary Telephones	Maximum Number of Bridged Extensions on Primary Phones
V3000	250	250	1200
V3000	More than 250	400	1200
V5000	250	250	1200
V5000	More than 250	400	1200

Table 22 Maximum Bridged Extensions

System	Device Limit	Maximum Number of Primary Telephones	Maximum Number of Bridged Extensions on Primary Phones
NBX 100	200	100	300

There are no restrictions on the number of secondary telephones or the number of bridged extensions on secondary telephones.

Provided that you do not exceed the limits shown in Table 22, you can configure the maximum number of bridged extensions using any combination of primary telephones and bridged extensions. For example, on a V5000 system, you can configure 400 primary telephones with three bridged extensions each or 300 primary telephones with 4 bridged extensions each to reach the limit of 1200.

You can configure a different number of bridged extension buttons on a primary and an associated secondary telephone. For example, if a primary telephone has 5 bridged extensions, you can configure one of the secondary telephones to have fewer (1 through 4) bridged extensions. However, if all of the primary bridged extensions are in use, the person at the secondary telephone will not be able to see all the calls.

You can define any one telephone as either a primary telephone or a secondary telephone, but not both. If the telephone has an Attendant Console associated with it, the bridged extension functions for the telephone extend to the Attendant Console. For example, you can configure an 3Com 2101 Basic Telephone with an associated Attendant Console as a primary telephone with up to 11 bridged extensions on Attendant Console buttons.

You can configure bridged extensions on the same buttons that are used for the telephone's extension or on non-extension buttons. Before you can create a bridged extension on a telephone, unlock the button settings for the telephone group to which the telephone belongs (click *Telephone Configuration* > *Telephone Groups*, select a group and then click the Button Mapping tab).

You can view a report that lists the primary and secondary telephones on which you have defined bridged extensions. See "Viewing Bridged Extension Information" on page 107.

When you define bridged extension appearances on a primary telephone:

- Incoming calls appear on the bridged extension buttons first, followed by the buttons (if any) associated with the primary telephone's extension. For example, by default, buttons 1, 2, and 3 are extension appearances of the primary telephone. If you define buttons 4, 5, 6, and 7 as bridged extensions on the primary telephone, incoming calls appear on primary telephone buttons in the order 4, 5, 6, 7, 1, 2, 3.
- Any bridged extension appearance that overlaps one of the defined extension appearances for the primary telephone take precedence over those extension appearances. For example, if you define buttons 3, 4, 5, 6, and 7 as bridged extension appearances on the primary telephone, incoming calls appear on primary telephone buttons in the order 3, 4, 5, 6, 7, 1, 2.

Example Bridged Extensions Configurations

Example 1: An 3Com Business Telephone, extension 1044, is defined as a primary telephone and buttons 2, 3, and 4 are defined as bridged extension buttons. Two other 3Com Business Telephones, extensions 1055 and 1066, are defined as secondary telephones on which extension 1044 appears. On the 1055 telephone, buttons 10, 11, and 12 are configured as the three bridged extension buttons for the 1044 telephone. On the 1066 telephone, buttons 4, 5, and 6 are configured as bridged extension appearances.

If a call is made to extension 1044, it can be answered using any of the following buttons:

- Extension 1044 (primary telephone) — button 2
- Extension 1055 (secondary telephone) — button 10
- Extension 1066 (secondary telephone) — button 4

In this example, both secondary telephones use buttons 1, 2, and 3 as extensions appearances for their own extensions.

Example 2: A 3Com Business Telephone with extension 1077 is defined as a primary telephone and buttons 4, 5, 6, 7, and 8 are defined as bridged extension buttons. Two other 3Com Business Telephones (extensions 1088 and 1099) are defined as secondary telephones on which extension 1077 is to appear. On the 1088 telephone, buttons 10, 11, and 12 are configured as bridged extension buttons. On the 1099 telephone, buttons 3, 4, 5, 6, and 7 are configured as bridged extension appearances for extension 1077.

If a call is made to extension 1077, it can be answered using any of the following buttons:

- Extension 1077 (primary telephone) — button 4
- Extension 1088 (secondary telephone) — button 10
- Extension 1099 (secondary telephone) — button 3

Secondary telephone 1099 has only two extension appearances for the 1099 extension because button 3, by default an extension appearance for the local telephone, has been used as a bridged appearance of extension 1077.

The primary telephone has buttons 1, 2, and 3 as local appearances of its own extension (1077). If multiple calls arrive at this telephone, they appear on buttons 4, 5, 6, 7, and 8, followed by 1, 2, 3.

Buttons 1, 2, and 3 on the 1077 telephone are not defined as bridged extension appearances. Therefore, they do not appear on either of the secondary telephones. If the owner of the 1077 telephone makes a call using any of these buttons, there is no indication (status light) of the call on either secondary telephone. If there are five active calls on the 1077 telephone, and a sixth call is made to that extension, it rings only on the 1077 telephone, on the first unused button in the 1, 2, 3 group).

Defining Bridged Extensions

The process of defining bridged extensions involves:

- Defining Bridged Extensions on a Primary Telephone
- Defining Bridged Extensions on a Secondary Telephone

Defining Bridged Extensions on a Primary Telephone

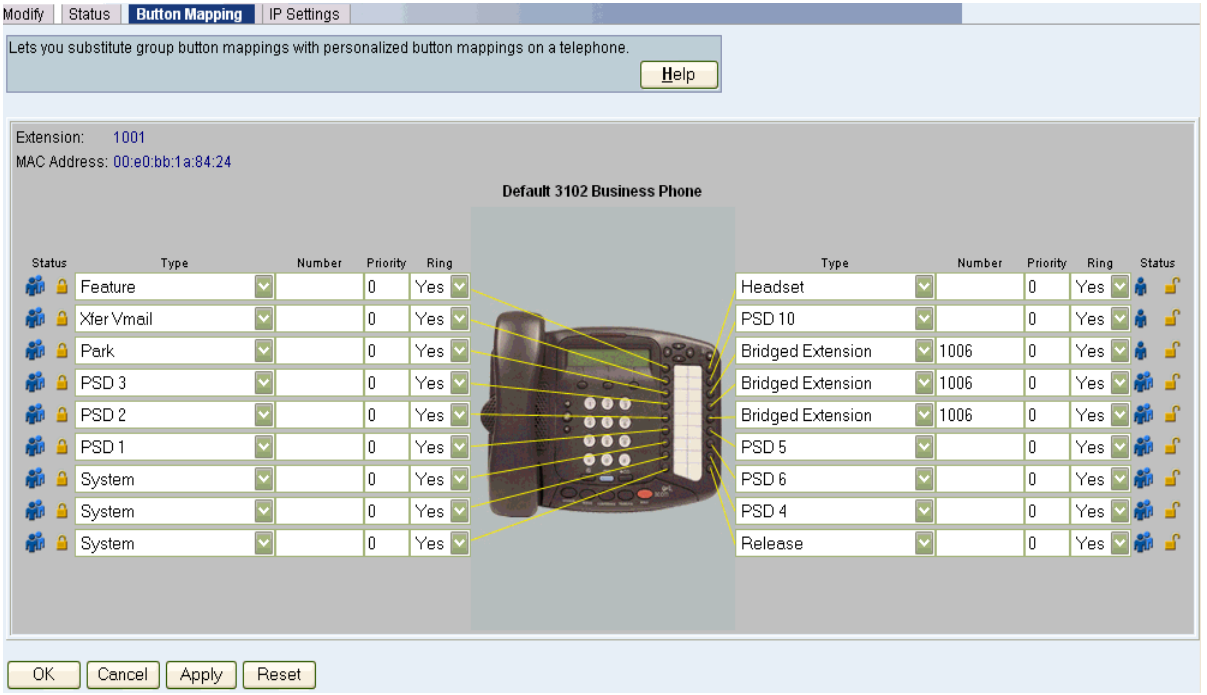
On a primary telephone, you can define from 1 to 11 buttons as bridged extensions. The buttons do not have to be next to each other.

Defining a bridged extension for a 3Com 3130 Manger's Telephone differs from other telephones. See "Defining Bridged Extensions on 3103 Manager's Telephones" *on* page 103 *for more information.*

To define the bridged extensions for the primary telephone:

1. Click *Telephone Configuration* > *Telephones*.
2. Click the extension for the primary telephone.
3. Click the *Button Mapping* tab to display the Button Mapping window (Figure 4).

Figure 4 Telephone Button Mappings Window



4 For each button that you want to include in the group of bridged extension buttons:

   a Select *Bridged Extension* from the drop-down list in the *Type* column.

   b Type the extension number of the primary telephone in the *Number* column.

   Figure 4 shows a group of three buttons that have been configured as bridged extension appearances for the extension (1066) on the primary telephone.

5 Click *OK*.

Defining Bridged Extensions on a Secondary Telephone

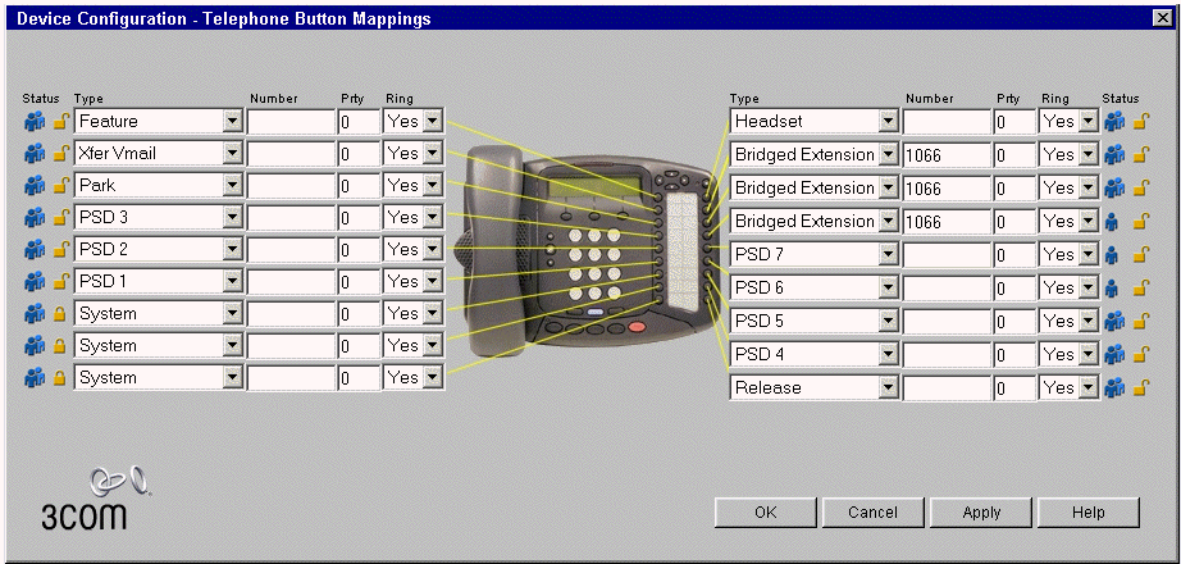
After you have defined the bridged extension buttons on the primary telephone, you can define the corresponding bridged extension buttons on a secondary telephone. You can do this for as many secondary telephones as you want.

To define the bridged extensions for a secondary telephone:

1. Click *Telephone Configuration* > *Telephones*.
2. Click the extension for the secondary telephone.
3. Click the *Button Mappings* tab to display the Button Mapping window.
4. For each button that you want to include in the group of bridged extension buttons:
   a. Select *Bridged Extension* from the drop-down list in the *Type* column.
   b. Type the extension number of the primary telephone in the *Number* column.

   Figure 5 shows a group of three buttons that have been configured as bridged extension appearances for the extension (1066) associated with the primary telephone.

Figure 5 Button Mapping Window After Mapping



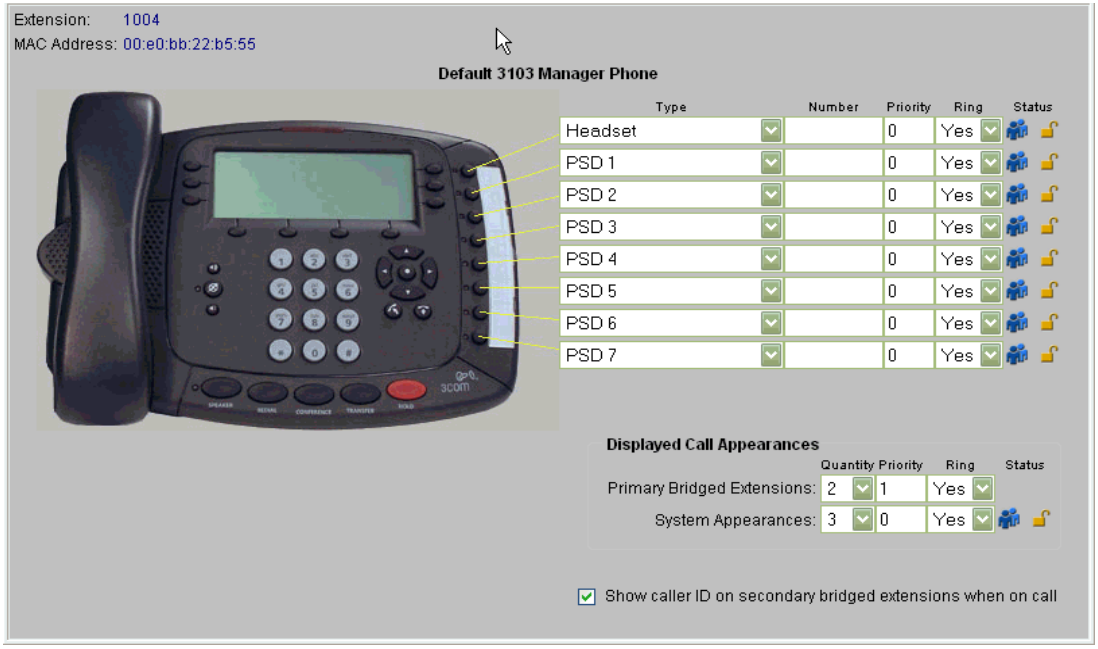
5. Click *OK*.

Defining Bridged Extensions on 3103 Manager's Telephones

To configure the 3Com 3103 Manager's Telephone as a secondary telephone and map a button as a bridged extension button, use the Type drop-down list, as you would for any other phone. The maximum number of button mappings for secondary bridged appearances is 8 (one per button).

To configure the 3Com 3103 Manager's Telephone as a primary telephone, you do not need to map primary bridged extensions to a button. Use the Displayed Call Appearances section of the Button Mapping window to configure the telephone (See Figure 6).

Figure 6 Telephone Button Mapping Window for 3Com 3103 Manager's Telephone



- From the Primary Bridged Extensions Quantity drop-down list, choose the desired number of primary bridged extensions, which also defines this telephone as a primary telephone. The maximum number of primary bridged appearances and system appearances, which you define from the System Appearances Quantity drop-down list, cannot total more than 12.
- From the System Appearances Quantity drop-down list, choose the number of system appearances for the telephone. The default number of system appearances is 3. The maximum number of system appearances and primary bridged extensions cannot total more than 12.
- Click the check box *Show caller ID on secondary bridged extensions when on call* check box so that this primary telephone's extension

displays on the secondary telephones with which it is associated. If you disable this option, the bridged extension button on the secondary telephone lights, however, the display panel does not display a Caller ID.

The telephone's display panel can display three system or bridged extension appearances, which are mapped to the buttons to the left of the display panel.

By default, bridged extensions have priority over system appearances. To give system appearances priority, change the priority of the primary bridged extension to a higher value. The lowest value in the priority field provides the highest priority.

Example: If you configure the primary telephone for a total of three system appearances and no bridged extensions, when all three lines are in use, a fourth call does not display in the display panel and goes directly to voice mail.

Example: If you configure the telephone for three system appearances and one bridged extension, a call to the primary telephone uses the bridged extension line and can be answered by associated secondary telephones. Any other calls to the primary telephone use the system appearance lines and cannot be answered by associated secondary telephones. If all three lines are in use, a fourth call causes the Message Waiting Indicator on the primary telephone to flash, but the display panel does not display any information. However, you can answer the call on the unused system appearance line. You can also make a call on an unused line.

Example: If you configure the telephone for three system appearances and two bridged extensions, the bridged extension lines take priority over the system appearance lines. If you make a call and put it on hold, and then make a second call, by default, both calls are on bridged extension lines. Because both bridged extensions are in use, any calls to the primary telephone are on system appearance lines, and cannot be answered by associated secondary telephones.

Example: If you choose two primary bridged extensions and give them a priority of 1 and choose one system appearance and give it a priority of 0, the system appearance will have the higher priority. When you make a call, by default, the call is on the system appearance line. This ensures that calls to the primary extension are on bridged extension lines and are

available to associated secondary telephones. If all three lines are in use and you make a fourth call, that call is on a bridged extension line.

Modifying Bridged Extensions

You can modify bridged extensions on a primary telephone at any time. Bridged extensions do not need to be on adjacent buttons on a primary or a secondary telephone. You can have a different number of bridged extensions on a primary and a secondary telephone.

Sample Calling Situations Using Bridged Extensions

This section describes typical telephone call situations involving bridged extensions on primary and secondary telephones. For all the examples:

- The primary telephone is an 3Com Business telephone (extension 1027) used by a manager (Alicia). This telephone has buttons 2, 3, and 4 defined as bridged extension buttons. Button 1 is the manager's private line.
- One secondary telephone, a 3Com Business Telephone (extension 1051), is used by the manager's assistant (Bradley). On this telephone, buttons 1, 2, and 3 are extension appearances for extension 1051 and buttons 4, 5, and 6 are configured as bridged extension appearances of the manager's telephone (1027).
- The other secondary telephone is also an 3Com Business Telephone (extension 1018). The telephone is used by the person (Connie) who answers the manager's telephone whenever the manager's assistant is not available. Buttons 10, 11, and 12 are configured as bridged extension appearances of the manager's telephone (1027).

Example 1: If there are no active calls on Alicia's telephone, a call made to her telephone from either an internal or outside telephone rings on button 2 on her telephone, button 4 on Bradley's telephone and button 10 on Connie's telephone.

Bradley answers the call by pressing button 4. After identifying the person who is calling, Bradley places the call on hold and informs Alicia of the call. Alicia presses button 2 on her telephone to take the call.

During the time that Bradley is talking to the caller, neither Alicia nor Connie can access the call. Alicia can pick up the call only after it is placed on hold by Bradley. Similarly, after Alicia picks up the call, neither Bradley nor Connie can access the call. If Alicia wants to include either Bradley or Connie in the call, she can set up a conference call.

Example 2: Alicia wants to place a call but wants to keep all three bridged extensions available for incoming calls. Alicia can place the call using button 1.

Neither Bradley's telephone nor Connie's telephone shows any indication that there is a call on Alicia's telephone, because button 1 on Alicia's telephone is not configured as a bridged extension.

Example 3: Three incoming calls have arrived on Alicia's telephone (on buttons 2, 3, and 4). Alicia is talking on button 2, Bradley has placed the second call on hold, and is talking to the third caller.

A fourth call arrives at Alicia's extension and rings on button 1. Neither Bradley nor Connie can answer this call because that button on Alicia's telephone is not a bridged extension appearance.

If a fifth call arrives at Alicia's extension before the fourth call stops ringing, it is sent directly to Alicia's voice mailbox, because all buttons are being used.

Example 4: A call arrives at Alicia's telephone and the building has been evacuated because of a fire. Neither Alicia, nor Bradley, nor Connie is available to answer the call. After the number of rings that are configured for Alicia's telephone, the call is sent to Alicia's voice mailbox.

Example 5: A call arrives at Alicia's telephone and Bradley answers the call, then places it on hold, and Alicia picks up the call. Bradley leaves the area, asking Connie to answer his telephone and Alicia's until he returns.

Alicia places the call on hold in order to pass the call back to Bradley but finds that he is not available. Connie is not close enough to Alicia's office to permit Alicia to talk directly to her, so Alicia presses another button on her telephone, calls Connie's extension, and asks her to pick up the call.

Viewing Bridged Extension Information

You can view a list of all telephones on the system and determine which are primary telephones and which are secondary telephones.

To view the bridged extensions information, click *Telephone Configuration* > *Telephones,* and click *Bridged Extensions*, which displays the NBX Bridged Extensions Report.

If a telephone is a primary telephone, the Bridged Extensions column contains the extension of the telephone and the extension of each

associated secondary telephone. The Mapped Buttons column displays the telephone's extension once for each button that is mapped as a bridged extension.

Example: If extension 1002 is a primary telephone and extensions 1005, 1008, and 1019 are secondary telephones with 1002 mapped to them, the Bridged Extensions column contains four extension numbers (1002, 1005, 1008, and 1019). If 3 buttons on the 1002 telephone are mapped as bridged extensions, the Mapped Buttons column contains extensions 1002, listed 3 times.

Camp On Feature and Bridged Extensions

There are some restrictions when you use the Camp On feature with primary bridged extensions.

You cannot initiate Camp On with Call Transfer to queue a call to an idle primary bridged extension line if the primary telephone user is on a call on the default system appearance line. The system treats the Camp On attempt as a blind transfer and routes the call to voice mail if the call is not answered.

However, you can initiate Camp On with Call Transfer to queue a call to a busy primary bridged extension line.

You can initiate Direct Camp On to queue a call to a busy primary bridged extension, regardless of which line is in use. That is, the primary telephone user can be using a system appearance line or a bridged extension line.

Creating and Managing Telephone Groups

Telephone groups let you create common button mappings, which let you assign specific actions to the buttons on an 3Com Business Telephone. When you associate a group with a specific telephone, the telephone inherits all the mappings of the group.

For example, when you use the NBX NetSet utility, you can create a group called Sales that includes access buttons mapped to a set of CO lines. When you add a new salesperson to the group, you specify the Sales group for the telephone assigned to that person. All of the Sales group's button mappings are then available on that person's telephone.

This section describes these topics:

- Creating a New Telephone Group

Creating a New Telephone Group

To create a new telephone group:

1. Click *Telephone Configuration* > *Telephone Groups*.
2. Click *Add*.
3. Type the name of the new group in the *Group Name* field.
4. Select an entry from the *Telephone Type* drop-down list.
5. To enable call recording and monitoring as the default setting for all telephones in this group, enable the *Call Record & Monitor* check box.

You must install a call recording license before you can enable the Call Record & Monitor *check box.*

6. Click *OK*.

   The Telephone Groups list includes the new group.

Modifying a Telephone Group

You might want to change the name of a telephone group to reflect a change in your organization, or you might want to change whether the group is configured for call recording and monitoring.

To change the name of a telephone group:

1. Click *Telephone Configuration* > *Telephone Groups*.
2. Click the group whose name you want to change.
3. Change the name of the telephone group in the *Group Name* field.
4. To set call recording and monitoring as the default condition for all telephones in this telephone group, enable the *Call Record & Monitor* check box.

You must install a call recording license before you can enable the Call Record & Monitor *check box.*

5. Click *OK*.

Removing a Telephone Group

You can remove a telephone group if you no longer need it.

To remove a telephone group:

1 Click *Telephone Configuration* > *Telephone Groups*.

2 Select the group, or groups you want to delete and click *Remove Selected*. To select all groups, enable the *Select* check box.

3 Click *OK* when the system prompts you to remove the group.

Viewing Telephone Group Membership

You can view a report that describes to which telephone group a telephone belongs. The report also includes membership information about Class of Service groups.

To view the membership report, which includes information about all telephone groups:

1 Click *Telephone Configuration* > *Telephone Groups*.

2 Click *Membership*.

3 Click any of the column headings to arrange the information in ascending or descending order.

Recording and Monitoring Telephone Calls

If you have call recording application software that runs on a PC that is external to the system, you can record and monitor telephone calls to and from telephones on the system.

To enable call recording and monitoring on the system, you must purchase a system-wide license. After you install the license, you can enable call recording and monitoring for these devices:

- Analog telephones connected to ports on an Analog Terminal Card or to a single-port Analog Terminal Adapter

  For instructions about how to enable these features, see:

  - "Adding an Analog Terminal Card" on page 125
  - "Adding an Analog Terminal Adapter (ATA)" on page 127
  - "Modifying an Analog Terminal Port" on page 127

- 3Com Telephones

  For instructions about how to enable these features, see:

  - "Adding a New Telephone" on page 93
  - "Modifying a Telephone" on page 95

- Telephone Groups

  For instructions on enabling these features, see:

  - "Creating a New Telephone Group" on page 109
  - "Modifying a Telephone Group" on page 109

Recording Calls Between Telephones with Different Recording Settings

For a call that involves 3Com telephones or analog telephones that are connected to either ATC ports or to ATAs, the system verifies the current recording setting for each device to determine which recording setting to use for the call.

Two-party Calls

In a two-party call involving only NBX devices, when you enable recording on either device, the system enables recording for both devices for the duration of the call. When the call has been completed, the system restores the recording settings that were in effect prior to the call.

Conference Calls

If you enable recording on any NBX device in a conference call, the system enables recording for all NBX devices for the duration of the conference call. When the call has been completed, the system restores the recording settings that were in effect prior to the call.

Example:

A three-party conference call involves these telephones:

- A 3Com Business Telephone on the local system
- An analog telephone connected to an ATC port on the local system
- A 3Com Basic Telephone on a different system, connected to the local system by a virtual tie line (VTL)

Only the 3Com Basic Telephone has recording enabled. For the duration of the conference call, the system enables recording for the analog telephone and the 3Com Business Telephone. After the call ends, the system disables the recording for the analog telephone and the 3Com Business Telephone.

Remote Telephones

If a 3Com telephone or an analog telephone connected to an ATA is connected to a subnetwork different than the Call Processor's, you can enable recording for that remote device.

Music On Hold (MOH)

On an NBX system, MOH is always recordable. During a call with two devices (3Com telephones, or analog telephones attached to ATC ports or to ATAs) that both normally have recording disabled, if either person puts the call on hold, the system enables recording while MOH is playing. When the call is taken off hold, the system restores the recording settings that were in effect prior to the call. If you disable MOH for the system, recording is not enabled while the call is on hold.

The MOH feature is available on Layer 2 devices only.

Non-3Com Telephones

If your system has telephones other than 3Com Telephones attached, you can include these telephones in 3Com telephone groups, provided that the other telephones are configured to emulate a 3Com telephone.

CAUTION: *If a telephone other than an 3Com Telephone is configured to emulate an 3Com telephone, then you can add the telephone to the associated telephone group (for example, the Default Business Phone Group). However, the other telephone might only partially emulate an 3Com Business Telephone and might not respond to the commands to enable or disable call recording. If you disable recording for the Default Business Phone Group, it might still be possible to record calls involving the telephones that are not 3Com Telephones in that group.*

Creating and Managing Button Mappings

Button mappings allow you to place features, such as speed dial numbers and shortcuts, on telephone buttons for individual telephones or for telephone groups. In addition, you can use button mappings to map CO telephone lines to buttons and set up your system in one of these modes:

- **Key Mode system** — In Key Mode, all outside lines map to individual buttons on users' telephones. You can share lines by assigning one line to multiple telephones. Incoming calls ring on all telephones that have that line assigned. Any of those telephones can answer the call.
- **PBX (Private Branch eXchange) system** — In a PBX system, outside lines are pooled and arbitrated by the Call Processor. To call an outside number, a telephone user must dial the line pool access number, typically 9, and the Call Processor assigns the next available line.
- **Hybrid Mode system** — In hybrid mode, some lines are assigned as keyed lines, while the rest are pooled.

You must use 3Com Business Telephones to operate the system in key mode or hybrid mode. 3Com Basic Telephones operate in PBX mode only.

This section describes these topics:

Mapping Access Buttons

3Com Telephone access buttons have these characteristics:

- 3Com 3101 and 3101SP Basic Telephones each have four Access buttons. Only two buttons can serve as line appearances, primary or secondary bridged station appearances, or any other feature. You cannot map the other two buttons as line appearances or primary bridged station appearances, but you can map any other feature to these buttons. These two buttons are mapped by default as Transfer and Feature, and changing these default mappings can limit the features you can access.
- On 3Com 1102, 2102, and 1102-IR Business Telephones, you can assign CO telephone lines or line pool access only to buttons that have lights. You can assign one-touch actions such as Speed Dial or system features such as Do Not Disturb to any access button.
- 3Com 2101 Basic Telephones include three access buttons. 3Com 2101 Basic Telephones operate in PBX mode only, that is, you cannot map CO lines directly to telephone buttons.
- Not all button type functions are available on all models of telephones. Functions that you might assign to a button include
- Camp On, Conference, WhisperPage, or Other, which lets you assign any feature code to a button. For a description of each function you can assign to a button, see the online Help.
- The use of the *Priority* (priority) and *Number* fields depend on the selected button type function.
- The *Ring* field is used to enable and disable ringing for a lone appearance button and to set delayed ringing patterns. See "Creating a Delayed Ringing Pattern" on page 115 for more information.
- A *Lock* check box at the Group Mappings level lets you control button inheritance behavior. If you lock a button at the Group Mappings level, a change made to the group always passes to every telephone in the group. If you clear the *Lock* box at the Group Mappings level, you

can override the mapping at the device level. An icon at the device level indicates whether the button can be remapped.

- The check box *Show caller ID on secondary bridged extensions when on call* appears on Button Mappings for the 3Com 3103 Manager's Telephone. This feature allows the device to display Caller IDs for bridged extensions.
- Telephone button mappings are part of a device. You assign a set of mappings to an individual by associating a particular device or group to the telephone user.
- Telephone users can see the button mappings in effect for their telephones by accessing the NBX NetSet interface with a personal password.
- Telephone users can use the NBX NetSet interface to create and print labels for the access buttons on their telephones.

Mappings for Telephone Users and Groups

When you create a new telephone users and assign them to a group, the button mappings for that group become active for the users' telephones. You can override group mappings and create mappings for individual telephones. For example, you can create a group called Sales and assign three shared direct lines to the group. Then you can assign one unshared direct line to each of the telephones currently in use by members of the Sales group.

The Lock feature (see "Creating Groups and Button Mappings" on page 116) allows you to control button behavior. If you enable Lock, a change that you make at the group level passes to every telephone in the group and it cannot be overridden for individual telephones. If you disable Lock, you can override group button mappings at the device level. (This Lock feature is not the same as the Telephone Locking feature that a telephone user can apply to an individual telephone. See the NBX Telephone Guide for more information.*)*

Creating a Busy Lamp/Speed Dial Button Mapping

A Busy Lamp/Speed Dial button is an access button, with a light, that is mapped so that it can function as a speed dial to another extension and also indicate when that extension is in use. When you press the access button mapped to the Busy Lamp/Speed Dial button, you dial the mapped extension. When the other extension is in use, the lamp lights on your telephone.

For the Attendant Console, the Auto Discovery process creates a default configuration that includes Busy Lamp/Speed Dial mappings for the first 100 extensions on the system.

A CO line mapped directly to telephones (Key mode) is not transferred to any telephone user's voice mail. For more information about key mode, see Creating and Managing Button Mappings on page 112.

To create a Busy Lamp/Speed Dial button mapping:

1. Click *Telephone Configuration* > *Telephones.*
2. Click a telephone extension.
3. Click the *Button Mapping* tab.
4. Select an available Access button that has a light.
5. From the *Type* drop-down list, select `Line/Extension`.
6. From the *Number* drop-down list, specify the extension of the telephone that you want as the Busy Lamp/Speed Dial target.

Creating a Delayed Ringing Pattern

You can define a ringing progression for a line that you map to multiple telephones. For example, you can configure a call to ring immediately at telephone 1, begin ringing at telephone 2 after 4 rings, and then begin ringing at telephone 3 after 8 rings. Any of the telephones can pick up the call at any time, even if it has not yet started audibly ringing at a particular telephone. (The light flashes during all rings.)

Delayed ringing works with Key mode only, that is, with line card ports mapped to buttons on two or more telephones.

To create a delayed ringing pattern:

1. Use the *Group Button Mappings* feature of the NBX NetSet utility to map a CO line. See Creating and Managing Button Mappings on page 112.
2. Set *Ring* to *Yes*.
3. Clear the *Lock* check box.
4. Click *Telephone Configuration* > *Telephones*.
5. Click the extension of the second telephone in the progression of telephones where you want to create the Delayed Ringing pattern, and then click the Button Mapping tab.

6 For the shared line appearance button, set the *Ring* box to the behavior that you want.

For the telephone to begin ringing after one ring, select `1`; after two rings, select `2`. Select `No` to disable ringing entirely. (The indicator light still functions to indicate ringing/call status.) Do not change the settings in the *Type*, *Number*, and *Prty* fields.

7 Repeat the procedure for each telephone in the Delayed Ringing pattern. Make sure you set the Ring delay to create the appropriate delay for each extension.

Delayed Ringing Notes

- Delayed ringing is useful for backup coverage on shared lines, such as for assistants who must cover each other's lines.
- The first telephone and each succeeding telephone in a delayed ringing pattern continue to ring until the call is answered or transferred to the Auto Attendant.
- Telephones belonging to a delayed ringing pattern do not need to belong to the same group. As long as all the telephones have the same line mapped, you can create the delayed ringing pattern.

Creating Groups and Button Mappings

Telephone button mappings are part of a device. You assign a set of mappings to an individual by associating a particular device or group to that telephone user.

A telephone user can see the button mappings in effect for an assigned telephone by logging on to the NBX NetSet utility with a personal password. The telephone user can also use the NBX NetSet utility to modify certain button mappings, and to create and print labels for the access buttons on the telephone and set up One-Touch Speed Dials.

An administrator can define the button mappings for telephone groups and also define exceptions to the group mappings for individual telephones.

To create groups and button mappings:

1 Click *Telephone Configuration* > *Telephone Groups.*

2 Click *Add*, type a *Group Name*, and click OK.

3 Click the telephone group name to which you want to apply mappings.

4 Click the Button Mapping tab.

5 See the online help for more information about how to configure the button mappings.

To define button mappings for an individual telephone:

1 Click *Telephone Configuration > Telephones.*

2 Click the telephone extension to which you want to apply mappings.

3 Click the Button Mapping tab.

4 See the online help for more information about how to configure the button mappings.

Changing Device IP Settings

If you are using Standard IP network protocol, you can manually change the IP address of telephones, Line Card ports, Attendant Consoles, and Analog Terminal Cards. You modify the IP settings of a device if you plan to move the device to a different subnetwork than that on which the Call Processor resides. If a DHCP server serves the new subnetwork, the IP address you assign to the device must be outside the address range that the DHCP server uses.

You can install 3C10116D T1 and 3C10165D E1 Digital Line Cards in a remote location and communicate with their Call Processors over a routed network. For a description about how to configure remote Digital Line Cards, see *"Setting Up a Digital Line Card at a Remote Location" on page 183*.

See the online Help for more information about IP network protocols.

The BRI and ATC/ALC daughter cards on the 3C10164D-ST share the same IP address. Therefore, depending on the configuration, you can change the IP address following these paths:

- Click *PSTN Gateway Configuration> Digital Line Cards,* click a MAC address, and then click the IP Settings tab.
- Click *Telephone Configuration > ATA*, click an extension, and then click the IP Settings tab.

If you change the IP Address for any of the daughter cards, the IP address of the other daughter cards changes as well. You can use this method only when the Call Processor and the 3C10164D-ST are located on the same Ethernet segment.

To change the IP settings of a telephone:

1 Click *Telephone Configuration > Telephones.*

If you are updating the IP Settings of a different type of device (such as an Attendant Console or a Digital Line Card), click the appropriate tab.

2 Click the extension of the telephone that you want to update.

3 Click the IP Settings tab.

4 Type the new values for IP Address, Subnet Mask, and Default Gateway address in the fields.

5 Click *OK*.

6 Disconnect the device from the Call Processor subnetwork.

7 Connect the device to the new subnetwork as follows:

- Connect a telephone or a single-port ATA to a port on either a switch or hub that is connected to the new subnetwork.
- Plug a card into a chassis that is connected to the new subnetwork.

8 Reboot the device:

- Remove power from a telephone or a single-port ATA, and then reconnect it.

  If the device is a card, it reboots automatically when you insert it into the new chassis. You do not need to remove power to the chassis when you add or remove cards.

When you change IP Settings, the system terminates all current calls through this device.

9 In the NBX NetSet utility, return to the IP Settings window for the device.

10 Verify that the device now reports the IP settings that you entered.

CAUTION: *If you configure an 3Com telephone for operation on a subnetwork other than the Call Processor's subnetwork, and if you access the* IP Settings *window to verify that the device settings are correct, click* Cancel *to exit the window. If you click* OK*, the system applies the IP settings in the* Manually Assigned IP Settings *fields. By default, all these fields contain 0.0.0.0. If you click* OK*, all the IP settings for the telephone are set to 0.0.0.0, and the telephone no longer works on the* remote *subnetwork.*

Configuring the Attendant Console

The Attendant Console provides extended button mappings and displays the current status of each extension mapped to it. A receptionist typically uses the Attendant Console to connect incoming calls to telephone extensions.

This section describes how to configure the Attendant Console manually. Alternatively, you can use Auto Discovery to add and configure the device automatically, and then use the manual configuration procedures in this section to fine-tune your mappings.

Before you autodiscover the Attendant Console, first autodiscover all telephones, Analog Terminal Adapters, and Analog Terminal Cards. The Auto Discovery process maps all existing telephones to the Attendant Console.

You can associate any 3Com telephone with an Attendant Console. However, if you use a 3Com 3103 Manager's Telephone, you cannot map a CO line directly to a button on the Attendant Console and the Attendant Console will not support Bridged Station Appearances.

This section describes these topics:

Adding an Attendant Console

Before you add Attendant Consoles, note the following requirements:

- On a V3000, V3001R, or V5000 system, you can configure up to 100 Attendant Consoles.
- On an NBX 100 system, you can configure up to 50 Attendant Consoles.

You can associate, at most, three Attendant Consoles with any one telephone.

The 3Com 3105 Attendant Console requires a license. You must enter a valid device license key into the NBX NetSet utility before you can add a 3Com 3105 Attendant Console to the system.

To add a new Attendant Console:

1. Click *Telephone Configuration* > *Attendant Console*.
2. Click *Add*.
3. Complete in the fields and make the appropriate selections for the new Attendant Console.
4. Click *OK*.

Modifying an Attendant Console

This section describes how to modify an existing Attendant Console. You can change an Attendant Console's device number or associated telephone. You must associate every Attendant Console with a telephone.

To modify an existing Attendant Console:

1. Click *Telephone Configuration* > *Attendant Console*.
2. Click the extension of the Attendant Console that you want to modify.
3. Modify the appropriate settings.
4. Click *Apply* to make the changes and then click *OK*.

Viewing Attendant Console Status

From the Attendant Console Status window, you can check the status of an Attendant Console. You can also reboot the Attendant Console from this window.

To view the status of an Attendant Console:

1. Click *Telephone Configuration* > *Attendant Console*.
2. Select the Attendant Console extension for which you want to view the status.
3. Click the Status tab.
4. View the settings and optionally change the Dialog Refresh, Device Refresh, and Reset Device settings. See the online Help for more information about these fields.
5. Click *Apply* to apply the settings and then click *OK*.

Removing an Attendant Console

To remove an Attendant Console from the system:

1. Click *Telephone Configuration* > *Attendant Console*.
2. Select the Attendant Console, or Attendant Consoles, that you want to delete and click *Remove Selected*. To select all Attendant Consoles, enable the *Select* check box.
3. Click *OK* in the dialog box to confirm.

Configuring Attendant Console Buttons

This section describes how to configure the buttons on the Attendant Console. The Attendant Console buttons include:

- 50 Access buttons. You can assign each button two settings.
- A Shift button. This button switches between the two settings allowed for each Access button.
- Four Feature buttons.

Configuring Feature Buttons

To map the Attendant Console Feature Buttons:

1. Click *Telephone Configuration* > *Attendant Console*.
2. Click the Attendant Console extension for which you want to map Feature Buttons.
3. Click the Feature Mapping tab.
4. Use the drop down list next to each button to select the feature you want to assign to the button.

   For a description of each function you can assign to a button, see the online Help.
5. Click *Apply* to implement the new mappings.

Mapping the Attendant Console Access Buttons

To map the Attendant Console Access buttons:

1. Click *Telephone Configuration* > *Attendant Console.*
2. Click the Attendant Console extension you want.
3. Click the Button Mapping tab.
4. To map the buttons that you want, follow these steps:
   a. Select the appropriate column of buttons. Click *1-50* to select columns A through E, or *51* through *100* to select columns F through J. (This

choice emulates the function of the *Shift* button on the physical Attendant Console.)

b Click the letter (*A* through *J*) that corresponds to the column of buttons that you want to map.

c Map the buttons for the column that you selected using the drop-down list boxes.

For a description of each function you can assign to a button, see the online Help.

5 Click *Apply* for the changes to take effect.

You cannot map a TLIM line or a primary bridged station appearance to an Attendant Console button if that Attendant Console is associated with a 3Com 3103 telephone. The 3Com 3103 Telephone display can show a maximum of 12 calls only, and there is no way to access any more calls at one time.

Changing Attendant Console IP Settings

Although most configurations use IP On-the-Fly or DHCP to assign IP addresses (and thus cannot manually change the addresses), if you use Standard IP network protocol, you can manually change the IP address of Attendant Consoles and other devices.

To set Attendant Console Feature IP settings:

1 Click *Telephone Configuration > Attendant Console*.

2 Click the extension of the Attendant Console

3 Click the IP Settings tab.

4 Type the new values for IP Address, Subnet Mask, and Default Gateway address in the fields.

5 Click *OK*.

When you change IP Settings, the system terminates all current calls through this device.

Configuring Connectivity to a 3105 Attendant Console Through the Serial Port

The 3Com 3105 Attendant Console supports manual configuration through the serial port on the underside of the device. You can specify the device's IP settings.

To connect the 3Com 3105 Attendant Console to a serial port on your computer requires the use of an adapter, such as the *Kentrox DE9S to EIA-561 (RJ45 SOCKET) ADAPTER MFR# 78909*. Other manufacturers

might offer appropriate adapters. The adapter you choose must use the pinout configuration shown in Table 23.

Table 23 Pinouts for 3105 Serial Connection

RJ45 pin	DB9 pin	Function
1	9	RI
2	1	DCD
3	4	DTR
4	5	GND
5	2	RXD
6	3	TXD
7	8	CTS

To connect a computer to the serial port on a 3105 Attendant Console:

1. Connect the DE9S to EIA-561 adapter to a serial port on the computer.
2. Connect a straight CAT5 cable (no crossover) from the RJ45 connector on the adapter to the **SERIAL 10101** port on the underside of the 3105 Attendant Console.
3. Start terminal emulation software on the computer and create a new connection.
4. Configure the connection to use the settings in Table 24.

Table 24 Terminal Emulation Program Properties

Property	Value
Emulation	VT100
Baud Rate	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

5. Use the commands in Table 25 to configure the 3Com 3105 Attendant Console. Make sure you specify IP and MAC address information appropriate for your network. Note that NCP refers to the Call Processor.

   For example:

   ```
   nbxSetIpAddress 192.168.123.123
   ```

```
nbxSetNcpMacAddress 00:eo:bb:11:a1:b4
```

Hyperterminal commands are case-sensitive.

Table 25 Hyperterminal Commands for Configuring the 3105 Attendant Console

Parameter	Hyperterminal Command	Comment
Device IP Address	`nbxSetIpAddress <nnn.nnn.nnn.nnn>`	Sets the IP address of the device. You clear the address is you set the IP address to 0.0.0.0 or 255.255.255.255.
Subnet Mask	`nbxSetSubnetMask <nnn.nnn.nnn.nnn>`	Sets the IP subnet mask for the device.
Default Gateway	`nbxSetGatewayAddress <nnn.nnn.nnn.nnn>`	Sets the IP address of the device's default gateway. You clear the address is you set the IP address to 0.0.0.0 or 255.255.255.255.
NCP IP Address	`nbxSetNcpIpAddress <nnn.nnn.nnn.nnn>`	Sets the IP address of the device's Call Processor. You clear the address is you set the IP address to 0.0.0.0 or 255.255.255.255.
NCP MAC Address	`nbxSetNcpMacAddress <##:##:##:##:##:##>`	Sets the MAC address of the device's Call Processor. Setting to clears the address. You clear the address is you set the MAC address to ff:ff:ff:ff:ff:ff.

You must also use the NBX NetSet utility to add the device to the system database.

Connecting and Managing Analog Devices

An Analog Terminal Card (ATC) or an Analog Terminal Adapter (ATA) allows ordinary analog (2500-series compliant) telephones, including cordless telephones and Group-3 facsimile (fax) machines, to operate with NBX systems.

These limitations apply due to the differences between an analog device and a 3Com Telephone:

- A telephone user dials 500, then ** on a telephone connected to an ATA to gain access to voice mail.
- An analog telephone can make or receive only one call. The system forwards a second incoming call to voice mail.

This section discusses these topics:

- Adding an Analog Terminal Card

- Adding an Analog Terminal Adapter (ATA)
- Modifying an Analog Terminal Port
- Removing an Analog Terminal Adapter
- Viewing The Status of an Analog Terminal Adapter

Adding an Analog Terminal Card

To add an Analog Terminal Card to the system using Auto Discovery:

1. Click *System-Wide Settings* > *Auto Discovery*.
2. Click the *Auto Discover Other Devices (including ATA, Digital Line Cards & Analog Line Cards)* check box.
3. Click *Apply*.
4. Insert the Analog Terminal Card into the chassis.
5. Wait approximately 1 minute for the system to discover the card.
6. Click *Telephone Configuration* > *ATA*.

   The four ports of the Analog Terminal Card appear in the ATA list, as well as the ports of any previously discovered Analog Terminal Cards and any previously discovered Single-Port Analog Terminal Adapters (ATAs).

Extension Assignments (3C10117 ATC)

The 3C10117C Analog Terminal Card replaces the 3C10117 Analog Terminal Card.

Each of the four ports on a 3C10117 Analog Terminal Card has a MAC address. The first port has the same MAC address as the card, and the remaining three ports have sequential MAC addresses incremented by one hexadecimal digit. See Table 26:

Table 26 MAC Addresses of Analog Terminal Card Ports (3C10117)

Card or Port	MAC Address
Analog Terminal Card	00:e0:bb:00:f8:c8
Port 1	00:e0:bb:00:f8:c8
Port 2	00:e0:bb:00:f8:c9
Port 3	00:e0:bb:00:f8:ca
Port 4	00:e0:bb:00:f8:cb

The extensions that the system assigned to these ports might not be in order. For example, if the system assigns extensions 7258, 7259, 7260, and 7261 to the ATC ports, it might assign 7258 to port 3.

To determine which extension is associated with a given port, click *Telephone Configuration* > *ATA* and examine the list of ATAs and ATC ports. For example, to determine the extension assigned to the third port, look for the ATC port with a MAC address that is two hexadecimal digits higher than the MAC address of the board. The extension of the port is in the first column (Extension).

After you add the Analog Terminal Card, you can configure the parameters for each of the four ports. See "Modifying an Analog Terminal Port" on page 127.

Extension Assignments (3C10117C ATC)

On a 3C10117C Analog Terminal Card, there is only one MAC address. Each of the four ports is assigned a unique virtual device number (1 through 4) so that the system software can address each port separately.

When you click *Telephone Configuration* > *ATA* to view the information, the system displays the port number, enclosed within square brackets, after the MAC address. See Table 27.

Table 27 MAC Addresses of Analog Terminal Card Ports (3C10117C)

Card or Port	MAC Address
Analog Terminal Card	00:e0:bb:00:f8:c8
Port 1	00:e0:bb:00:f8:c8[1]
Port 2	00:e0:bb:00:f8:c8[2]
Port 3	00:e0:bb:00:f8:c8[3]
Port 4	00:e0:bb:00:f8:c8[4]

The extensions that are assigned to these ports by the system might not be in order. For example, if the system assigns extensions 7258, 7259, 7260, and 7261 to the ATC ports, it might assign 7258 to port 3.

To determine the extension assigned to any port on a 3C10117C ATC:

1. Click *Telephone Configuration* > *ATA*.
2. Look for the combination of MAC address and port number that you want. The extension associated with the port is in the first column (Extension).

After you have added the Analog Terminal Card, you can configure the parameters for each of the four ports. See "Modifying an Analog Terminal Port" on page 127.

Adding an Analog Terminal Adapter (ATA)

To add an Analog Terminal Adapter (ATA) to the system:

1. Click *Telephone Configuration* > *ATA*.
2. Click *Add.*
3. Complete the fields, as necessary. See the online Help for more information.
4. Click *Apply* to add the new ATA to the system.
5. Repeat as necessary to add more ATAs.
6. When you are finished adding ATAs, click *OK*.

Modifying an Analog Terminal Port

You can modify the configuration of an Analog Terminal Card port or a single-port ATA at any time.

To modify an analog device configuration:

1. Click *Telephone Configuration* > *ATA*.
2. Click the extension of the device that you want to modify.
3. Modify the fields, as necessary. See the online Help for more information.
4. Click *Apply* to effect the changes.
5. Click *OK*.

Removing an Analog Terminal Adapter

You can remove either an Analog Terminal Adapter (ATA) or one of the ports on an Analog Terminal Card (ATC) from the system at any time. Any device connected to the ATA is also removed from the system.

To remove an ATA or ATC port:

1 Click *Telephone Configuration > ATA*.

Use the MAC addresses to determine whether an item in the list is an Analog Terminal Adapter (ATA) or one of the ports on an Analog Terminal Card. Ports on a 3C10117 Analog Terminal Card have MAC addresses that differ by two hexadecimal digits. Ports on a 3C10117C Analog Terminal Card all have the same MAC address and use a Virtual Device Number to identify each port. The system displays a port number, enclosed in square bracket, after the MAC address. An ATA has a unique MAC address with no port number.

2 Select the ATA or ATC port that you want to delete and click *Remove Selected*. To select all ATAs or ports, enable the *Select* check box.

3 Click *Remove Selected*.

Viewing The Status of an Analog Terminal Adapter

You can view the status of either an ATA or one of the ports on an ATC at any time.

To view the status of an ATA or an ATC port:

1 Click *Telephone Configuration > ATA*.

Use the MAC addresses to determine whether an item in the list is an ATA or one of the ports on an ATC. Ports on a 3C10114 Analog Terminal Card have sequential MAC addresses. Ports on a 3C10114C Analog Terminal Card all have the same MAC address followed by a Virtual Device Number (VDN), enclosed in square brackets. An Analog Terminal Adapter has a unique MAC address with no port number.

2 Click the extension of an ATA or ATC port.

3 Click the Status tab.

4 View the device status and make any necessary changes. See the online Help for more information.

5 Optionally, to send a status message to the Call Processor about the ATA or ATC port, click *Refresh Device*.

6 Optionally, to reset the ATA or ATC port, click *Reset Device* and click *OK* when the system prompts you confirm.

CAUTION: *On the 3C10114 Analog Terminal Card, you can reboot individual ports without affecting the other ports. However, if you reboot a port on the 3C10114C Analog Terminal Card, all four ports on the card reboot, which disrupts active calls on any of these ports.*

7 Click *OK*.

Advanced Settings

You can set the audio gain and timing controls on an ATA or each port of an ATC. To set these parameters:

1 Click *Telephone Configuration* > *ATA*.

2 Click the extension of an ATA or ATC port.

3 Click the Advanced Settings tab. See the online Help for more information.

If you change any of the values in the Advanced Settings dialog box, the settings you change persist if you later upgrade the system software or you change the regional software.

6 User Configuration

This chapter describes these elements of the system:

- Users
- Phantom Mailboxes
- Class of Service (CoS)

For more information about these topics and configuration procedures, see the online Help.

Users

You use the Users window in the NBX NetSet utility to add telephone users and remove them from the system. You can also modify and maintain user profiles and parameters.

To perform these tasks:

1. Click *User Configuration* > *Users*.

To add a SIP telephone to a SIP-mode system, you must first add a SIP telephone user and extension to the system database, and then use the SIP telephone to complete the configuration.

2. See the online Help for information about how to add, modify, and remove telephone user settings, and about SIP telephones.

   For information about user settings that individual telephone users can configure, see Chapter 1 in the *NBX Telephone Guide*.

Phantom Mailboxes

A phantom mailbox is an extension that has no associated physical telephone. A caller can dial directly into a phantom mailbox and leave a message. The person assigned to a phantom mailbox can create and send a message from within the voice mail system and the Auto Attendant can route callers to a phantom mailbox.

Example: A telephone user who is never in the office can use a phantom mailbox to receive and manage messages, even though no telephone is associated with the mailbox extension. The telephone user can call into voice mail to retrieve and send messages, log onto the NBX NetSet utility to manage messages, including having the system forward voice messages using the Off-Site Notification feature, or use an e-mail client to manage the messages. See "IMAP for Integrated Voice Mail" in Chapter 9.

To create a phantom mailbox:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *User Configuration* > *Users*.
3. See the online Help for information about how to add, modify, and remove phantom mailboxes.

To access a phantom mailbox from any telephone, the telephone user:

1. Calls the extension.
2. Presses * during the greeting.
3. Logs in.
4. Provides mailbox initiation information when the system prompts, if this is the first time the phantom mailbox is accessed.
5. Use the NBX NetSet utility to set up telephone options, such as Call Forwarding, after setting up a password.

Class of Service (CoS)

Class of Service (CoS) is a set of calling permissions that you assign to telephone users. Most permissions are subject to the Business Hours parameters: Open, Lunch, and Other. For example, you can create a class that allows toll calls during normal business hours, but denies them at other times. You can control if the telephone user can use certain features, such as mapping features to buttons on the telephone or preventing a call from being monitored.

To configure CoS:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *User Configuration* > *Class of Service*.

3 See the online Help for information about how to add, modify, remove, and view Class of Service.

Note the following considerations:

- Emergency calls (such as calls to 911) are not subject to CoS restrictions.
- System-wide Speed Dial numbers are not subject to Class of Service restrictions. For example, if you want to enable calling to a specific toll number to all telephone users without regard to their CoS settings, create a System Speed Dial for that number.
- When you create a new profile, the system assigns the default CoS unless you specify a different one. If you edit the properties of the default CoS, verify that it contains a minimum set of permissions.
- You can enable or disable Off-site Notification at the system level. The system-wide setting takes precedence over the CoS setting.
- A telephone user can override the CoS of a telephone by using feature code 433. For example, a telephone user with an assigned office telephone that allows calls to external numbers needs to place a call to an external number from a conference room telephone with a CoS that does not allow external calls. The telephone user enters the feature code into the conference room phone, and the system prompts for username and password before allowing the call. The feature code applies to the next call only. After the telephone user hangs up, the telephone reverts to its assigned CoS.
- To set an account code as Forced, enable the *Force Acct Code* check box for each appropriate Class of Service (click *User Configuration* > *Class of Service*, and then click an extension or *Add*).

  Verifying account codes is a global configuration setting, while enforcing account codes is a CoS function. If the CoS setting enforces the account code for that type of call, a telephone user must enter an account code before the system routes the call.
- You can allow telephone users to configure button mappings on their own devices. Enable User Button Mappings when you add or modify a group's CoS settings. If you enable this feature, when the individual telephone user clicks *Telephone Programming* in the NBX NetSet utility, the system displays the Button Mapping tab, which enables the telephone user to map functions to telephone buttons. If you do not enable this feature, the system does not display the Button Mapping tab.

- If you allow telephone users to configure button mappings on their own devices, a telephone user can override any button mappings that you set unless you lock the button to prevent changes. To lock a button, click *Telephone Configuration* > *Telephone Group*s, and then select a telephone group and click the Button Mappings tab. The Button Mapping window includes *Lock* check boxes next to each programmable Access button. Enable the Lock check box to prevent telephone users from mapping a function to the selected button.
- CoS permissions do not apply to hunt groups. This means a CoS cannot prevent you from configuring operators in a Hunt Group.

Service classes control these types of calls:

- Intercom
- External (local, long distance, international, long distance toll-free, and long distance toll)
- CO Code (optional telephone company services, such as Call Waiting)
- Trunk to trunk transfers
- Off-site Notification
- Configurable operators (destinations pre-selected by the user to which callers are sent if those callers reach the telephone user's voice mail)

7 Call Distribution Groups

Call distribution groups allow for the distribution of incoming calls to the appropriate agent without any specific action on the part of that agent.

The system supports two kinds of call distribution groups:

- A *hunt group* is a set of telephone users that you can access when you dial a single extension
- An Automatic Call Distribution, or ACD, group is similar in concept and practice to a hunt group. However, an ACD group includes other features, such as database capabilities, that are specifically suited to call center operations.

Topics in this chapter include:

For more information about these topics and configuration procedures, see the online Help.

Automatic Call Distribution (ACD)

A call center is the general term that refers to any system that accepts incoming calls to a site, ensures that those calls are sent to the proper destination within the site, and manages database records on call activity and distribution. For example, you can use the call center as a help desk, a reservations counter, an information hotline, or a customer service center. A telephone call center typically manages collections of telephone extensions that are linked to a centralized database.

The ACD distributes calls to agents and queues the calls that have not been answered before a pre-determined time period expires. The ACD

also manages recorded announcements to callers, manages individual ACD agents and groups of agents, and provides database reports about both calls and agents.

The Call Pickup feature is supported for ACD groups.

Topics in this section include:

- ACD Groups
- ACD Shifts
- In-Queue Digit Processing and Announcements
- ACD Group Open/Close and Announcements
- Announcements for SIP-Mode Systems
- Wrap-Up Time
- Streaming ACD Data Through a TCP Socket

See the administrator online Help for configuration instructions.

ACD Groups

To take full advantage of ACD, organize your ACD agents into ACD groups. An ACD group is a number of agents that the system treats as a single entity for the purposes of handling calls.

- Supported ACD Group Types
- Multiple ACD Group Membership
- ACD Agent List
- ACD Licenses
- ACD Group Populations

Supported ACD Group Types

The system supports the following ACD group types:

- **ACD Linear Group**

  The system can distribute calls to the group in a linear fashion. An incoming call goes to the agent ranked first and, if the agent is not available, then to the agent ranked second. The process continues in this way until the system completes the rankings, at which point the call cycles to top of the rankings list to begin again.

- **ACD Circular Group**

The system can distribute calls to the group in a circular fashion. The system attempts to place an incoming call with the agent whose rank follows the agent that received the last call. If this agent is not available, the call goes to the next ranking agent. If the second agent is not available, the system from that point on treats the call as linear.

- **ACD Most Idle Agent Group (MIA)**

  The system can distribute calls to the group on the basis of idle time; that is, the system directs the call to the agent who has been idle for the longest amount of time, then to the agent that has been idle the next, longest amount of time. If the second agent does not answer the call, the system then treats the call as linear.

- **ACD Least Call Count**

  Least Call Count mode distributes calls to ACD agents based on the number of calls that those agents have answered in a defined period of time.

  In other words, the agent with the least number of answered calls for a given duration of time becomes the next available agent. For example, two agents in a group each have been logged in to their ACD group for ten minutes. Agent One, has answered five calls and Agent Two has answered ten calls. In this case, the system assigns Agent One to receive the next incoming call.

  All types provide a timeout value that determines final call handling, such as voice mail or Auto Attendant, if the timeout value is exceeded.

- **Calling Groups**

  A Calling Group is an ACD group in which a single call alerts or rings *all* member telephones. In this case, all the telephones in a Calling Group continue to ring until a member answers the call, or until the Total Timeout value is reached.

  The practical effects of this behavior are as follows:

  - The Per-device Timeout applies to every device in a Calling Group.
  - A Calling Group call alerts an agent's telephone that is busy or on another call *once*, then blinks on one of the System Appearance lines.
  - The system does not alert logged-out members.
  - Only one call is served out to the ACD queue. The other calls must wait to be served or routed to call coverage until after the Total Timeout value has been reached.

- If all Calling Group members are logged out, the system forwards the call to call coverage immediately.
- If there are no current members in the Calling Group, the system forwards the call immediately to the call coverage path.
- You cannot configure the system to log out an agent that does not answer automatically.

Multiple ACD Group Membership

If any agent is a member of more than one ACD group, the system tracks requirements such as Least Call Count and Most Idle Agent so that these requirements are taken into account when calls are routed to that agent.

For example, Agent One is a member of two ACD groups. Agent One's call count reflects the total of calls received from both groups, so Agent One's idle time reflects the total for calls that come from both groups. The system routes calls to Agent One based on this calculation.

You can use this feature to allow agents with different skill sets to be a part of multiple ACD groups.

ACD Agent List

Both ACDs and hunt groups act upon a list of selected extensions rather than the entire directory of telephone extensions on the system. In the case of ACD, the supervisor creates this list, called an Agent list.

The system does not support bridged station appearance behavior for ACD agents. When a bridged station appearance is added as an agent to an ACD group, the system routes incoming ACD group calls to the primary telephone only.

ACD Licenses

A software license determines the number of agents that you can add to the Agent list. The Base License key for ACD allows two agents. You can purchase an additional license that authorizes three more agents, for a total of five agents. Thereafter, you must purchase licenses to add agents by increments of five agents.

You may configure a maximum of 200 ACD agents for each system.

ACD Group Populations

ACD administrators typically organize agents whose functions are logically related into entities called ACD groups. These groups can be used instead or with the ACD Agent List while creating (or modifying) the ACDs. ACD groups can be added as members of the ACD along with the individual extensions from the ACD Agent List.

ACD Shifts

ACD can provide different kinds of work shifts for ACD agents. As well as managing calls, ACD shifts can differentiate work assignments in the Real-Time Streaming Statistics, and to reset internal statistics used by the Most Idle Agent and Least Call Count call distribution methods.

The ACD shift feature is not available on SIP mode systems.

You can set up an ACD group to have any one of the following shifts:

- **24-hour shift** – The ACD group always accepts incoming calls. This is the default behavior.
- **Shift that uses system business hours** – The ACD group uses defined business hours (click *System-Wide Settings > Business Hours)*.
- **One of four custom configurable shifts** – The ACD group uses the hours specified in the ACD function *Custom Hours*.
- **Dynamic or Emergency Shifts** – The operating hours of the ACD group are dynamically reset in the ACD function *Custom Hours*.

Custom Operating Hours and Shifts

ACD includes the concept of customizable work shifts. You plan your ACD call coverage at your site that best suits the call center. As the basis for this discussion, click *Call Distribution Groups > ACD Groups.* Then, click an extension or *Add*, and click the Custom Hours tab.

The Start time of a shift is the End time of its predecessor. However, you do need to specify the Start time and End Time for each appropriate day because this is what defines the operating boundaries of the ACD for that day.

- Shift 1 is mandatory, and represents the start of operations.
- Shifts 2,3 and 4 are optional, and you need only enter the Start time for those shifts.

The system routes any call to the ACD within the operating hours to its agents. Any call that arrives outside the ACD operating hours generates a Closed announcement, and the system forwards the call to preconfigured call coverage.

Dynamic or Emergency Shifts

If an ACD is closed, you can force it into an Open state to accept calls during an emergency (click *Call Distribution Groups* > *ACD Groups* and then click *Open/Close*).

Designate the start of shift as the time of the Force Open action. All statistics for Least Call Count and MIA begin from this Force Open Start time. The End time for this dynamic or emergency shift is either the Start time of the next shift or the Force Close time, whichever happens first.

Estimated Wait Time Announcements

You can configure the system to provide recorded announcements that inform the caller approximately how long it will be before an agent answers the call. For example, you can record an announcement such as "An agent will take your call in approximately one minute. Please stay on the line."

This time interval is called Estimated Wait Time. The system uses both static and dynamic information to calculate Estimated Wait Time. To designate an announcement as an Estimated Wait Time Announcement, click *Call Distribution Groups* > *ACD Groups*, click an extension or *Add*, and then click the Announcements tab.

Estimated wait time announcement is not supported in SIP-mode systems at this release.

In-Queue Digit Processing and Announcements

While a call is in the ACD queue, the calling party can press a digit to force the system to take the call off the queue and forward it to the Call Coverage path. You configure this In-Queue Digit Hot Key in the *Announcements* window. (The default digit is '#'.)

The Call Coverage path can be one of the following:

- Call coverage path of the ACD group itself (default)
- Auto Attendant
- ACD Voice Mailbox

- Another extension (another ACD, Hunt Group, internal extension, extension over VTL, or external number)

Make the caller aware of this ability to break out of the call queue by recording an in-queue digit announcement, then designating the .WAV file as such in the *In-Queue Digit Announcements* section of the *Announcements* window.

In-Queue Digit processing (including its associated announcements) is not supported in SIP-mode systems at this release.

ACD Group Open/Close and Announcements

An ACD Group is considered Closed at any time other than the configured shifts (business hours). However, you can provide an announcement (using the Announcements window) that provides the reason why the ACD group is closed. The system then forwards the call to Call Coverage, using the same path as that designated in Group Time Out.

You can force the Close state (click Call Distribution Groups > ACD Groups *and then click* Open/Close*) of any ACD Group for a holiday or emergency. You must manually enable the first thing on the next working day. Any new calls after the force close receive an ACD close announcement and the system forwards them to call coverage. In case of a force open, the ACD closes at the next configured close time.*

Announcements for SIP-Mode Systems

A SIP-mode system uses a different audio codec format than a system that uses 3Com call control. If you are running in SIP mode, you must use an IP messaging server (such as the 3Com IP Messaging Server) instead of NBX Voice Mail Messaging.

A system running in SIP mode does not support estimated wait-time announcements or In-Queue Digit Processing.

Wrap-Up Time

Wrap-Up Time is the time interval needed by an agent in this ACD group to take notes on or follow up a completed call. During Wrap-Up Time, the system routes no calls to the agent except personal calls or Calling Group calls.

The timer value is specified in seconds, and the Wrap-Up timer engages after the agent completes the ACD call. The display panel or status light on the agent's telephone indicates that Wrap-Up Time is engaged. After

Wrap-Up-Time expires, the agent becomes available to take new calls, and the display panel or status light deactivates.

You can set the Wrap-Up timer value between 0 and 999 seconds. A zero value (default) signifies that Wrap-Up Time is not configured.

The Wrap-Up Time feature is not available on SIP mode systems.

Wrap-Up Time Indicators

The status light associated with the button mapped for Wrap-Up Time lights up while the agent is in Wrap-Up mode. This status light turns off after Wrap-Up time is complete, or when the agent overrides it.

In addition to the status light, the display panel displays `Wrap Up` during the time allotted, then returns to the default display after the Wrap-up time is complete, or when the agent overrides it.

Wrap-Up Time Agent Override

Feature code **972**, or a mapped button, allows the agent to override the Wrap-Up timer to take new calls immediately.

However, the agent can override the Wrap-Up timer only after completing the call. This means that even if the agent wants to override Wrap-Up time during an ACD call to take another ACD call, the agent cannot do so. The only exceptions to this rule are personal calls or Calling Group calls.

Therefore, if an agent is part of two ACD Groups, the agent cannot receive calls from either group if Wrap-Up Time has engaged after an ACD call from either group. After the timer expires and the agent takes a call from the second ACD group, closing this call starts the Wrap-Up Timer from the second ACD group, which the agent can override.

Wrap-Up Time Agent Extend

Agents who need extra Wrap-Up time can map another button, or use Feature Code **973** to extend this time. The agent can only extend while Wrap-Up time is active; once the Wrap-Up time expires, the agent cannot extend the wrap-up time. An agent can extend Wrap-Up time one instance by default.

Streaming ACD Data Through a TCP Socket

You can use the NBX NetSet utility to enable one TCP port to stream ACD data from the system to an external device for further analysis. (The NBX ACD Desktop Statistics Application from 3Com provides the client-side support for this data streaming. See your authorized reseller for details.)

NBX 100 systems do not support streaming ACD data.

Any number of ACD groups can share this port. The data can be enclosed in XML tags to facilitate parsing at the client side or, alternatively, can be streamed in pure text or ASCII format as name value pairs. This data stream contains detailed data for all of the ACD groups and their agents.

ACD Considerations

Make sure you are aware of these restrictions before you configure ACD operations on your site.

- Hardware Limits for ACD Groups
- ACD Operations With Call Detail Reports (CDR)
- Display Data
- Voice Mail Port Usage

Hardware Limits for ACD Groups

Table 28 lists the limits on the number of ACD groups for each hardware platform:

Table 28 ACD Group Limits

Systems	Limit
■ V3001R (128 MB) ■ V3000 (128 MB) ■ NBX 100V5000	Up to 48 concurrent ACD groups
■ V3001R (640 MB) ■ V3000 (640 MB) ■ V5000	Up to 100 concurrent ACD groups

ACD Operations With Call Detail Reports (CDR)

The Call Detail Reports application creates a Microsoft Access database for the data that it extracts from the system. This database has only one table, and all data is put into this table.

For ACD calls, the CDR application puts all call data into a new, second table. The fields in this table differ from the other table and, therefore, provide more details about the ACD calls.

The ACD group table data is accessible by CDR, but hunt groups do not have this table.

ACD reports in the CDR Application

The CDR client application has been modified to give you the option of viewing the new table for the ACD groups. Also, CDR provides pre-defined reports for ACD groups that ACD supervisors are able to use for performance evaluation.

Display Data

The ACD windows do not refresh themselves, you must manually refresh the window to see the latest data.

Voice Mail Port Usage

On a system with NBX Voice Messaging enabled, ACD announcements use system voice mail ports. The following platform limitations for voice mail ports apply:

- 72 voice mail ports (V3000, V3001R, and V5000 systems)
- 12 voice mail ports (NBX 100 systems)

See the section "Contention" on page 151 for more information about resource limitations for delayed announcements.

Using ACD

First, determine the scope of your call center operations. Then determine that you have the system resources that you need:

- Less than the allowable maximum of devices on the system
- Sufficient number of voice mail ports
- Sufficient number of ACD licenses (one for each agent)

Next, allot the agents into ACD groups, and decide how many agents within each group that you need. Once you reach the point where your call center planning is complete, you can begin to configure ACD operations.

The ACD user interface is set up such that you can configure ACD as soon as your planning is complete. Click *Add* in ACD Groups window to configure each group. This button invokes a configuration utility that leads you through the configuration process: defining ACD group

characteristics, identifying group agents, defining announcements for the group, and summarizing the group creation process.

After you have set up the ACD group or groups, you can configure other settings to assist their operation, including feature mappings and Supervisory Monitoring Domains (*Feature Settings > Supervisory Monitoring*). You can also modify your configuration settings.

ACD Groups

The ACD Groups feature allows you to configure the relationship between agents and groups.

The following sections provide information about the fields and buttons in the ACD Groups window (Click *Call Distribution Groups > ACD Groups*).

Display Fields in the ACD Groups Window

Table 29 describes what each display field shows in the ACD Groups window.

Table 29 ACD Groups window: Field Description

Field	Description
Extension	Lists the extension that the administrator assigned to this ACD group.
Name	Lists the name that the administrator assigned to this ACD group.
Method	Shows the call distribution method that the administrator assigned to this ACD group. Types include: ■ Linear ■ Circular ■ Most Idle Agent ■ Least Call Count ■ Calling Group
Members	Shows the number of extensions associated with this ACD group.
State	Whether the group is Open or Closed.

Functions on the ACD Groups Window

The ACD Groups window allows you to configure the operating environment of the ACD groups at your site. You can perform specific

group-related tasks, such as adding a group, modifying a group password, or removing an agent from a group.

Table 30 describes the functions that you can access from the ACD Groups window.

Table 30 Function on the ACD Groups Window

Function	Description
Add	Invokes a multi-step configuration utility that helps you create a new ACD group.
Modify	Click a Group Extension to change the configuration parameters of an existing ACD group.
Memberships	Lists the data of agents in a specific ACD group
Announcements	Provides the means to add, change, remove and list the audio files used for the recorded greetings in an ACD group.
Remove	Deletes an existing ACD group.
Status	Provides a snapshot report of a selected ACD group.
Feature Mappings	Provides the means to list or change the feature codes mapped to ACD extensions.
Supervisory Monitoring	Configures the settings for Supervisory Monitoring, a facility that allows a supervisor to monitor calls to agents. See "Supervisory Monitoring" for more information.
Off-Site Notification	Allows you to forward calls to specific telephone numbers outside the ACD facility.

For more information about the configuration procedure, see the online Help.

ACD Announcements

ACD plays audio announcements to parties that call the ACD site. You create or import these announcements as .WAV files so that callers waiting to speak to an ACD agent hear an audio message of your choice. You can configure up to five different ACD announcements for each ACD group.

ACD announcements work for ACD groups only; hunt groups do not have this feature. For SIP-mode systems, you must configure ACD Announcements through the IP Messaging Service. See Chapter 10 for more information.

Announcement Sequence

The system plays the first announcement file after the caller has been in the queue for the time delay specified in the **Time Interval** field (Click *Call Distribution Groups* > *ACD Groups*, click an extension or *Add*, and the click the Announcements tab).

The system plays the remaining files as the time interval for each file expires (assuming the caller is still in the ACD queue waiting to be connected to an agent). This means that you can set up the sequence in which announcements are played, with a predefined time delay between them, to engage the caller. In between announcements, the caller hears Music-On-Hold.

After the system plays all the announcements that you configured for the ACD group, the system plays the last announcement repeatedly (as per the time interval specified for it) during the rest of the wait period: that is, until the call is answered or until the ACD group's timeout period is exceeded. If the timeout period is exceeded, the system forwards the call to the destination that you specified in the **Group Coverage Action after Timeout:** field when you added or modified the ACD group.

If the agent answers the call, the system immediately stops playing the announcement, or the Music-On-Hold, and connects the caller to the appropriate agent.

Fields in the Announcements Window

Table 31 describes the function of each field and button in the Announcements window (Click *Call Distribution Groups* > *ACD Announcements)*.

Table 31 Announcements Window: Field Descriptions

Field	Description
(List of WAV Files)	Displays a list of .WAV files currently known to ACD.
Record	Records a .WAV file for an ACD announcement. You must have .WAV recording capability on the workstation you are currently using.
Play	Plays back the .WAV file that you selected from the list of WAV files.
Remove	Deletes the .WAV file that you selected from the list of .WAV files.

Table 31 Announcements Window: Field Descriptions

Field	Description
Play/Record Extension	Lets you identify the telephone extension to which the selected .WAV file applies.
Apply	Associates the .WAV file that you identified in the Play/Record Extension.
Enter the New Announcement Name to Record	Lets you associate a mnemonic name with the .WAV file.
Enter Path for .WAV File to Import Announcement	Lets you point ACD to the location in the file system of the .WAV file that you want to associate with the selected telephone extension.
Browse	Instructs the system to search the file system under your direction for the .WAV file to associate with the selected telephone extension.
Import	Imports a .WAV file from the file system into the ACD list of usable announcements.

ACD Agents

The Agent List window allows you to display the status of each ACD agent.

The statistical data does not contain the details for the ACD agents; the display shows the overall summary of the ACD activity at that instance.

Fields in the Agent List Window

Table 32 describes the function of each field and button in the Agent List window (Click *Call Distribution Groups > ACD Agents)*.

Table 32 Agent List Window: Field Descriptions

Field	Description
Extension	Displays the telephone extension of the agent.
First Name	Displays the first name of the agent.
Last Name	Displays the last name of the agent.
Status	Identifies the current telephone status of the agent. Categories include: Connected - The agent's telephone is offhook. Idle - The agent's telephone is onhook. Ringing - The agent's telephone is ringing.

Table 32 Agent List Window: Field Descriptions

Field	Description
DNIS	Indicates whether the system is using Dialed Number Identification Service (DNIS) to identify the caller to this agent.
ANI	Indicates whether the system is using Automatic Number Identification (ANI) to identify callers to this agent.
Call	Indicates whether the call that the agent is engaged in is an ACD call or a non-ACD call.

Agent Edit List Window

You can add an agent to or remove an agent from the list of valid ACD agents.

To assign a system user as an ACD agent, do the following:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *Call Distribution Groups* > *ACD Agents*.
3. Click the Edit List tab.
4. Click *Show All* to display a list of available telephone users.
5. Click the select box for the telephone user, or users, that you want to add to the Agent List.
6. Click *Apply*.

If the number of agents exceeds the number allowed by the license (five in the case of the Basic ACD license), the system disables the Add button and displays an error message to indicate that the maximum number of agents has been reached.

To unassign a system user as an ACD agent, do the following:

1. Click the Select box to deselect any user in the Agent List that you want to unassign from ACD responsibilities.
2. Click *Apply*.

ACD Statistics

The ACD Statistics window allows you to gather meaningful data about agents, calls, and callers to specific ACD groups.

As the administrator, you can either view the data for a selected ACD at a time, or view the data for all of the ACDs at the same time. The data viewed is a "snapshot" of the ACD at the discrete time at which you invoked the Statistics display.

Refresh the display to ensure that the data is current.

Fields in the ACD Statistics Window

Table 33 describes the function of each field and button in the ACD Statistics window. ACD Statistics also shows the Resource Contention statistics. (Contention occurs when the system does not have a port available to assign to an ACD group.)

Table 33 Statistics Window: Field Descriptions

Field	Description
Resource Report	Displays instances of contention.
Extension	Displays the telephone extension for this ACD.
Name of ACD	Displays the name of the ACD that is associated with this extension.
Logged In Agents	Displays the total number of agents logged in at the time you invoked the Statistics window.
Current Queue	Displays the number of calls that are currently in the call waiting queue of this ACD.
Answered Calls	Calls to this ACD that were answered since the last reset of the statistics facility.
Dropped Calls	Calls to this ACD that were dropped since the last reset of the statistics facility.
Total Calls	Total number of calls to this ACD group that have been received since the last reset of the statistics facility.
Last Reset Command Date	The date/time stamp at which the statistics facility was last reset (call counters reset to zero) for this particular ACD group.
Reset ACD Statistics	Resets the statistics facility to zero.
Reset ACD and Member Statistics	Resets the ACD and Member statistics, and updates the Last Reset Command Date field.

If the ACD has not reset since last system reboot, the system displays a null reset date value.

Contention

The system groups audio devices, such as voice mail ports, into a pool or extension list in the dial plan. It uses this extension list or pool for delayed announcements. The system selects an idle device from this list to play a delayed announcement. The number of devices in this pool is based on usage, and you can add or remove devices to suit the call volume.

On a system with NBX Voice Messaging, you can reserve NBX Voice Mail ports for Delayed Announcements to prevent Auto Attendant or voice mail applications from using the ports.

1. Create a new extension list and add the ports that you want to reserve (click *Dial Plan* > *Extension List*, and then click *Add*).
2. Delete those ports, which you added to the new extension list, from the default voice mail extension list (click *Dial Plan* > *Extension List*, and then click **0003*).
3. Edit the dial plan to include the new extension list (click *Dial Plan* > *Configure*, and then click *the Modify tab).*
4. Configure the appropriate ACD group to use the new extension list for Delayed Announcements:
   a. Click Call Distribution Groups > ACD Groups.
   b. Click the ACD group's extension.
   c. Click the Announcements tab.
   d. From the *Select a port to play announcements* drop-down list, select the new extension list.

The ports in the new extension list are now reserved and available exclusively for Delayed Announcements.

On a busy system, there can be an additional delay in the playing of an announcement. This condition can occur if all the audio resources (system voice mail ports) from the Delayed Announcement Audio Pool are in use.

If this delay occurs, the scheduled announcement must queue up for an audio resource to become available before it can be played to the caller. During that time, the caller either hears ring-back (when the system initially routes the call to the ACD Group for the initial announcement or greeting) or Music-On-Hold (if the caller has already heard a announcement, or the call is the result of a transfer or forward operation).

To avoid this problem, you can:

- Record or import announcements of short duration.
- Add more audio resources (system voice mail ports) to the Announcement Resource Pool.

The system records the instances of contention and displays them on the Resource Report window (click *Call Distribution Groups > ACD Statistics* and click the Resource Report tab).

Table 34 Resource Report: Field Description

Field	Description
Extension	Extension number associated with this contention event.
Name of ACD	Name of the ACD group that could not be assigned a port, causing the contention event.
Number of Occurrences	Number of times that the contention event occurred.
Most Recent Occurrences	List of the most recent occurrences of a contention event with this extension in this ACD group.
Extension List	List of agent extensions affected by the contention.
Refresh	Brings the Resource Report data up-to-date.

Hunt Groups

A hunt group is a set of telephone users that you can access when you dial a single extension. A call routed to the hunt group extension can reach any member of the group who is currently logged into the group. A static hunt group is one in which all members are permanently logged in (locked). A dynamic hunt group lets you log telephone users in to and out of the hunt group, or you can allow telephone users to log into or out of the group themselves, using the hunt group password you create.

You can associate one or more of the hunt group login/logout feature codes with a particular group and then map that feature code to a telephone access button to allow telephone users to easily login and logout of the hunt group. The access button light remains lit while the user is logged into the hunt group.

Hunt groups are specified by extension, in these ranges:

- **V3000, V3001R, and V5000 systems:** 4000–4099 (You can assign all 100 extensions.)

- **NBX 100 systems:** 450–499 (You can assign a maximum of 48 extensions.)

To configure hunt groups:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *Call Distribution Groups > Hunt Groups.*
3. See the online Help for more information.

To enable Supervisory Monitoring for a Hunt Group, define a Supervisory Monitoring Domain (click Feature Settings > Supervisory Monitoring*) that includes the Hunt Group.*

Hunt Group Considerations

- For a telephone to participate in a hunt group, the telephone user must be logged into the hunt group. See the *NBX Telephone Guide* for more information.
- You can lock in a member of a hunt group, which prevents the member from logging out of the system. See the online Help for more information.
- When you create a hunt group, you specify one of three types: **linear hunt group, circular hunt group,** or **calling group.** You base your choice on the ringing pattern that you want.
- For each group that you define, you also specify:
  - The **Total Timeout** — The length of time in seconds that the call rings on the group's telephones before the call goes to the group's call coverage point.
  - The **Per-Device Timeout** — The length of time in seconds that each telephone rings in the cycle. (Ignored for Calling Groups.)
  - Whether you want the system to log a telephone out of the hunt group if it does not answer. (Ignored for Calling Groups.)
- For linear and circular hunt groups, the *order* in which a group telephone rings (the telephone's priority) is the same as the order in which you added it to the group. For calling groups, all phones ring simultaneously.
- The Call Pickup feature is not supported for hunt groups.

Linear and Circular Hunt Groups

In linear and circular hunt groups, calls ring sequentially on telephones in the group, but the behavior differs when the time specified in the Total Timeout field elapses:

- If the Total Timeout value is less than the sum of all of the Per-Device Timeout values, a call that is routed to either a linear and circular hunt group rings on some, but not all of the telephones in the group and then is routed to the group's call coverage point.
- If the Total Timeout value is greater than the sum of the Per-Device Timeouts:
  - For a Linear Hunt Group, the call rings in order on each group telephone and then goes to the group's call coverage point. The system ignores any time remaining in the Total Timeout, and the call does not ring again on any telephone in the group.
  - For a Circular Hunt Group, the call rings in order on each group telephone and then, for the remainder of the Total Timeout, begins ringing again through the telephones, in order. Depending on the Total Timeout value, an unanswered call might ring through all telephones in the group multiple times.

If the Total Timeout value exactly matches the sum of the Per-Device Timeouts, the behavior of a single incoming call is the same for both linear and circular hunt groups.

When the system routes a second call to a linear or circular hunt group, the telephone on which the second call first rings is different:

- For a Linear Hunt Group, the new call rings on the first telephone in the group.
- For a Circular Hunt Group, the new call rings on the telephone that is next in the ringing sequence.

Calling Groups

In this special type of hunt group, an incoming call rings on all telephones in the group simultaneously. After the *Total Timeout* value is reached, a call that is still unanswered is routed to the group's call coverage point.

The value in the Per Device Timeout *field has no effect on the behavior of telephones in a calling group.*

Call Coverage

For each hunt group, you can define where the system routes an unanswered call (the call coverage point):

- **Voice Mail** — The system routes an unanswered call to the hunt group extension's voice mailbox or to a configured operator.
- **Auto Attendant** — The system routes an unanswered call to the Automated Attendant that you specify.
- **Phone Number** — The system routes an unanswered call to the extension that you specify, such as the receptionist, or another hunt group.

Hunt Group Supervisory Monitoring

You can configure the system to allow a privileged user to join an ongoing conversation in a hunt group with or without the knowledge of the parties involved in that conversation. This feature is called *Supervisory Monitoring*.

The monitoring user is called the *supervisor*. The supervisor, who might or might not be the system administrator, can join a call between a person calling into the system (for example, a customer) and a person on-site whose job it is to accept incoming calls. Joining calls in progress can ensure proper customer support.

To enable Supervisory Monitoring for a Hunt Group, you must define a Supervisory Monitoring Domain (*Feature Settings* > *Supervisory Monitoring*) that includes the Hunt Group. For more information about Supervisory Monitoring, see "Supervisory Monitoring" in Chapter 3.

8 PSTN GATEWAY CONFIGURATION

This chapter describes how to configure PSTN gateway devices on the system and addresses these topics:

- Configuring and Managing Analog Line Card Ports
- Configuring and Managing Digital Line Cards
- Setting Up a Digital Line Card at a Remote Location
- Setting Up T1/E1 Logging
- Viewing CSU State Information and Statistics
- Using Loopback Tests
- Obtaining a Dial Tone from a PBX System

For more information about these topics and configuration procedures, see the online Help.

For information about installing the system hardware components, see the NBX Installation Guide.

Configuring and Managing Analog Line Card Ports

Each Analog Line Card provides access for up to four local telephone lines into your system. The Call Processor treats a line card port as an extension, so each line card port needs its own extension number.

You use Auto Discovery to detect line card ports, and you define the starting address for Auto Discovery of devices in the system dial plan. For a 3-digit dial plan, the default starting address is 750; for a 4-digit dial plan, the default starting address is 7250. Auto Discovery assigns the first unassigned number, starting at 750 (or 7250 for a 4-digit dial plan), to the first line card port.

You typically configure line cards during installation. See the NBX Installation Guide *for more information.*

If you remove a line card from the system, the port information remains in the system database. The extension numbers assigned to the four ports do not become available for reuse unless you use the NBX NetSet utility to remove the line card from the configuration database.

This section describes these topics:

Configuring a Line Card Port

When you configure a line card port, you can assign it as a member of a line pool.

You can configure a line card port automatically (recommended) or manually.

Verify that you have chosen a 3-digit or 4-digit dial plan before you begin to configure line card ports. See Chapter 11 for information about how to configure the dial plan.

Configuring a Line Card Port Automatically

To configure a line card port automatically:

1. Login to the NBX NetSet utility using the administrator login ID and password.
1. Click *System-Wide Settings* > *Auto Discovery*.
2. Enable the *Auto Discover Other Devices (including ATA, Digital Line Cards & Analog Line Cards)* check box.
3. Click *Apply*.

Configuring a Line Card Port Manually

Most organizations use Auto Discovery to configure line card ports automatically. However, you can configure a line card port manually and select all settings.

To configure a line card port manually:

1. Click *PSTN Gateway Configuration* > *Analog Line Cards*.
2. Click *Add*.
3. Specify the port information. See the online Help for more information.
4. Click *OK*.
5. Connect your CO line to the configured port.

Auto Extension Behavior

The extensions you specify in the Auto Extension fields control where the system directs a call. Table 35 describes typical the behaviors for Auto Extension.

Table 35 Auto Extension Configuration

Button Mapping Setting for This Line	Auto Extension Setting	Incoming Call Behavior
Not mapped to any telephone	Extension of the Receptionist	Receptionist's telephone rings. If no one answers, the call transfers to the call coverage point defined for the Receptionist's telephone. The transfer occurs after the number of rings specified for the Receptionist's telephone.
Not mapped to any telephone	500	Calls go directly to the Automated Attendant without ringing any telephone.
Mapped to a button on the Receptionist's Telephone (or to a button on an Attendant Console associated with the Receptionist's telephone)	Extension of the Receptionist	Receptionist's telephone rings. If no one answers, the call transfers to the call coverage point defined for the Receptionist's telephone. The transfer occurs after these two values are surpassed: ■ The number of seconds specified in the *Time Out* field for the appropriate time of day (Open, Closed, Lunch, Other). Click *PSTN Gateway Configuration* > *Analog Line Cards* and click an extension. ■ The number of rings specified in the user settings for the Receptionist's telephone. **Example:** If the Time Out value for the Analog Line Card port is 12 seconds, the equivalent number of rings is 2. If the Call Forward settings for the receptionist's telephone is 4 rings, then the call transfers after 6 rings.

Table 35 Auto Extension Configuration (continued)

Button Mapping Setting for This Line	Auto Extension Setting	Incoming Call Behavior
Mapped to a button on the Receptionist's Telephone (or to a button on an Attendant Console associated with the Receptionist's telephone)	500	Receptionist's telephone rings. If no one answers, the call transfers to the Automated Attendant. **NOTE:** The call coverage point defined for the receptionist's telephone has no affect. The transfer occurs after the number of seconds specified in the *Time Out* field for the appropriate time of day (Open, Closed, Lunch, Other). Click *PSTN Gateway Configuration* > *Analog Line Cards* and click an extension.
Mapped to a button on a user telephone (or to a button on an Attendant Console associated with the user's telephone)	Extension of the Receptionist	User telephone rings. If no one answers, the call transfers to the Receptionist's telephone. The transfer occurs after the number of seconds specified in the *Time Out* field for the appropriate time of day (Open, Closed, Lunch, Other). Click *PSTN Gateway Configuration* > *Analog Line Cards* and click an extension. If the receptionist's telephone is not answered, the call transfers to the call coverage point defined for the receptionist's telephone.
Mapped to a button on a user telephone (or to a button on an Attendant Console associated with the user's telephone)	500	User telephone rings. If no one answers, the call transfers to the Automated Attendant. The transfer occurs after the number of seconds specified in the *Time Out* field for the appropriate time of day (Open, Closed, Lunch, Other). Click *PSTN Gateway Configuration* > *Analog Line Cards* and click an extension.

Modifying a Line Card Port

You can modify a line card port that is already configured.

To modify a line card port:

1. Click *PSTN Gateway Configuration* > *Analog Line Cards*.
2. Click the extension of line card port that you want to modify.
3. Specify the port information. See the online Help for more information.
4. Click *OK*.

Removing a Line Card Port

When you remove a line card port that is already configured, you remove the port information from the system database.

To remove a line card port:

1. Click *PSTN Gateway Configuration > Analog Line Cards*.
2. Select the extension, or extensions, of the line card port that you want to delete and click *Remove Selected*. To select all extensions, enable the *Select* check box.
3. Click *OK* when the system prompts you to confirm.

Verifying Line Card Port Status

You can verify the status of a configured line card port at any time.

To view the status of a line card port:

1. Click *PSTN Gateway Configuration > Analog Line Cards*.
2. Click the extension of the line card port.
3. Click the Status tab.
4. See the online Help for more information.

Rebooting a Line Card Port

To reboot a line card port:

1. Click *PSTN Gateway Configuration > Analog Line Cards*.
2. Click the extension of the line card port.
3. Click the Status tab.
4. Click *Reset Device*.

CAUTION: *On the 3C10117 Analog Line Card, you can reboot individual ports without affecting the other ports. However, if you reboot an analog port on the 3C10114C or 3C10114D Analog Line Card, the system reboots all ports on the card. This action can disrupt active telephone calls on any of these ports.*

Advanced Settings

The Advanced Settings window enables you to set the audio gain and timing controls on each port of an Analog Line Card.

To set these parameters:

1. Click *PSTN Gateway Configuration > Analog Line Cards*.
2. Click the extension of the line card port.
3. Click the Advanced Settings tab.

4 See the online Help for more information about the dialog box fields.

If you change any of the values in the Advanced Settings window, the settings that you change persist if you upgrade the system software or change the regional software later.

Configuring and Managing Digital Line Cards

This section describes how to add and configure these Digital Line Cards:

- **T1** Digital Line Card to connect to a T1 service that the local telephone company provides.

  You can configure the T1 Digital Line Card to use one of two types of signaling:

  - DS1 protocol (sometimes referred to as *Standard T1*)
  - ISDN PRI (Primary Rate Interface) signaling

    The system provides E911 (emergency) connectivity if the T1 Digital Line Card is configured for ISDN PRI signaling. The system provides the calling number (ANI) so that the emergency services personnel can determine the location of the caller from the E911 database. You must update the CO (PSAP) databases.

- **E1** Digital Line Card to connect to an E1 service that the local telephone company provides.

  You can configure an E1 Digital Line Card for ISDN PRI signaling only.

- **BRI-ST** Digital Line Card to manage a BRI line with four BRI spans using the ST interface.

  Each BRI-ST Digital Line Card (3C10164C or 3C10164D) supports the Basic Rate Interface protocol (ST interface only).

The Port, Channel, and BRI Group configuration instructions in this chapter apply to the 3C10164D Digital Line Card and to the BRI-ST ports on the V3000 BRI-ST, 3C10601A.

The 3C10164D is a gateway device capable of providing BRI-ST digital interfaces. The 3C10164D card supports eight BRI channels (four ports).

This section describes these topics:

- Modifying a Digital Line Card
- Adding or Modifying a Digital Line Card Group
- Modifying Card Channels
- Modifying IP Settings
- Removing a Digital Line Card

3C10165D E1 and 3C10116D T1 Digital Line Cards have expanded capabilities that are described in these topics:

- Setting Up a Digital Line Card at a Remote Location
- Setting Up T1/E1 Logging
- Viewing CSU State Information and Statistics
- Using Loopback Tests

Adding a Digital Line Card

To add a Digital Line Card to a system, use the information in these sections:

- Preparing the System for Digital Line Cards
- Ordering DID, CLIP, and MSN Services
- Enabling Auto Discovery for Digital Line Cards
- Inserting the Digital Line Card

Preparing the System for Digital Line Cards

Before you insert a:

- T1 Digital Line Card into the chassis, order a T1 line from your telephone carrier
- E1 Digital Line Card into the chassis, order an E1 line, with the specifications you want, from your telephone carrier
- BRI-ST Digital Line Card into the chassis, order an ISDN BRI-ST line from your telephone carrier

Have the telephone carrier install the line.

In some cases, the telephone company offers T1 services only with specific, pre-defined parameters. However, some telephone companies offer a number of configuration choices with their T1 services.

Ordering DID, CLIP, and MSN Services

When you order a:

- BRI line with DID (Direct Inward Dial) capability, Calling Line ID Presentation (CLIP), or MSN services
- E1 line with DID (Direct Inward Dial) capability, Calling Line ID Presentation (CLIP), or MSN services
- T1 line with DID (Direct Inward Dial) capability

the local telephone carrier assigns a block of telephone numbers to you. Usually, you can request a specific range of numbers, but sometimes the carrier assigns numbers other than the ones you request.

You might be able to request that the local telephone carrier pass you a specific number of digits for each incoming telephone call. Sometimes the carrier does not offer any choice. In either situation, you need to know how many digits the carrier passes.

Example: Carriers commonly pass either the last three digits or last four digits of the number for each incoming call.

Sometimes the last digits of the telephone numbers that the carrier assigns to you do not match the telephone extension numbers you want to use for internal calls. Create entries in your dial plan configuration file to trans- late the incoming numbers into the corresponding extension numbers.

Example: You want to use internal extensions from 4000 through 4999, but the local telephone carrier assigns you numbers from 617-555-3500 through 617-555-4499. You can create translator entries in the dial plan configuration file to translate an incoming digit sequence such as 3795 into extension number 4295, and a sequence such as 4213 into 4713. The configuration requires several translator entries to manage subsets of the total range. A unique set of entries would manage incoming digit sequences from 3500 through 3599, from 3600 through 3699, and each of the other sequences in which the first two digits were unique in the range from 37XX through 44XX.

If the DDI/DID (Direct Inward Dial/Direct Dial Inward) numbers match your internal extension numbers, the translator entries in your dial plan configuration file can be much simpler.

Example: You plan to use internal extensions from 100 through 299, and the local telephone company assigns you numbers from 617-555-4100 through 617-555-4299. If the local telephone carrier passes you three digits, you need no translator entries in the dial plan configuration file. If the carrier passes you four digits, you could add a single set of translator entries to the configuration file to remove the first digit (4) and use the remaining three digits as the internal extension.

Enabling Auto Discovery for Digital Line Cards

To enable Auto Discovery for Digital Line Cards:

1. Login to the NBX NetSet utility using the administrator login ID and password.
1. Click *System-Wide Settings > Auto Discovery*.
2. Enable *Auto-Discover Other Devices (including ATA, Digital Line Cards & Analog Line Cards)* check box.
3. Click *Apply*.

Other check boxes might be enabled based on previous Auto Discoveries. You do not need to clear these check boxes to install the Digital Line Card. However, it is good practice to clear all check boxes other than the one that you want to enable so that the Call Processor does not continue to search for added devices.

Inserting the Digital Line Card

You do not need to remove the power cable from the chassis before you insert the Digital Line Card.

To insert the Digital Line Card into the chassis:

1. Record the MAC address of the Digital Line Card.
2. Select a slot for the Digital Line Card in the chassis.
3. Insert the Digital Line Card into the slot.

   Slide the Digital Line Card into the chassis until you feel it touch the connectors.
4. To seat the Digital Line Card into the connectors, apply firm pressure to both the left and right sides of the front of the card.
5. Tighten the left and right screws on the front of the Digital Line Card to secure it to the chassis.
6. Wait 3 minutes.

CAUTION: *When you insert a Digital Line Card, it begins an initialization sequence that might include a firmware upgrade. Also, because you enabled the Auto Discovery feature, the system recognizes the new card and begins to update its database. Allow 3 minutes for these processes to complete.*

CAUTION: *The T1 Digital Line Card reboots twice during the initialization process. If you attach a console cable to the COM1 port on the T1 card and use Hyperterm software to view the text output from the card, you see status messages associated with the two reboot processes. See* *"Connecting a Computer to a Serial Port" on page 444*.

Another way that you can be sure that it is safe to proceed is to examine the status lights on the front panel of the T1 card. After the Auto Discovery process completes, and before you connect the T1 Digital Line Card to the telephone company's T1 line, the CF (Carrier Fail) light appears solid green on a 3C10116C card. On a 3C10116D card, the POST, DNLD, CARD and Call Processor lights appear solid green. For more information about T1 card status lights, see *"E1 and T1 Digital Line Card Status Lights" on page 171*.

You are now ready to configure the Digital Line Card.

Configuring the Digital Line Card

These sections tell you how to use the NBX NetSet utility to set up your Digital Line Card ports:

- Configuring the Digital Line Card
- Configuring Digital Line Card Groups
- Verifying Group Membership
- Completing the Configuration

Before you configure the Digital Line Card, see Chapter 11 for more information about how to configure the dial plan.

Configuring the Digital Line Card

CAUTION: *Before you begin to configure the Digital Line Card, make sure you wait 3 minutes after you insert the Digital Line Card into the chassis.*

To configure the Digital Line Card:

1. Login to the NBX NetSet utility using the administrator login ID and password.
2. Click *System-Wide Settings* > *Auto Discovery*.
3. Enable the *Auto Discover Other Devices (including ATA, Digital Line Cards & Analog Line Cards)* check box, if necessary.
4. Click *PSTN Gateway Configuration* > *Digital Line Cards*.

   The T1/ISDN Board List displays all Digital Line Cards (T1, E1, or BRI-ST) that the system discovers. the NBX NetSet utility refers to Digital Line Cards as either cards or boards.

By default, the Auto Discovery process selects DS1 as the signaling type for a T1 Digital Line Card.

5. In the *T1/ISDN Board List,* click the MAC address of the Digital Line Card that you installed into the chassis.
6. To change the name of the Digital Line Card, edit the contents of the *Board Name* field to identify the card in device lists.
7. For BRI service, verify that the *Card Type* field displays *ISDN BRI*. If it does not, the system has not properly autodiscovered the card. Restart the installation process.
8. To change the signaling type for a T1 Digital Line Card to ISDN PRI, select *ISDN PRI* from the *Card Type* drop-down list.

   To see the change, you might need to wait a minute or two, and refresh your browser window.
9. Enable the *On Line* check box.
10. Verify that the system lists all channels.

    The *Channel List* displays all channels. The channel numbers appear after the MAC address, separated by a hyphen.

    Example:

    2...00:01:03:48:e0:4e-2.... New Trunk.

    The 2 after the hyphen indicates channel number 2.

    Verify that system lists:

    - All 30 channels for an E1 board.
    - All 24 channels for a T1 board.

- The highest channel as 23 for a T1 ISDN PRI board.

  When you configure a T1 Digital Line Card for ISDN PRI signaling, one of the 24 channels is allocated for signaling, leaving 23 for data (voice).

11 Click *Apply*.

Connecting the Line and Activate the Span

1 Plug the line into the Digital Line Card.

For BRI service, use a category 5 Ethernet cable to connect the BRI interface box to one of the ports on the front panel of the BRI-ST card or the V3000 BRI-ST.

1 Click the appropriate link:

- *PSTN Gateway Configuration > T1 Spans*
- *PSTN Gateway Configuration > ISDN PRI Spans*
- *PSTN Gateway Configuration > ISDN BRI Spans*

2 Click the MAC address of a span.

3 Enable the *On Line* check box.

4 Click *OK*.

5 In the *T1/ISDN Board List*, verify that the entry for this card in the *Status* column changes from *Offline* to *Ready*. You might need to wait a minute or two, and then refresh your browser window to see this change.

For reports about all installed Digital Line Cards, click PSTN Gateway Configuration > Digital Line Cards*, and then click* Config. & Status Report *and* Export Report. *See* *"Digital Line Card Troubleshooting" on page 413* *for more information.*

Configuring Digital Line Card Groups

To configure the Digital Line Card groups:

1 Click the appropriate link:

- *PSTN Gateway Configuration > IT1 Groups*
- *PSTN Gateway Configuration > ISDN PRI Groups*
- *PSTN Gateway Configuration > ISDN BRI Groups*

2 Click the name of a group.

For T1 Digital Line Card groups, the fields in the Modify window contain default values. No default values are assumed for Called Party Digits or Calling Party Digits.

3 To modify the name of the group, enter a new name in the Group Name field. You can use alphanumeric characters, hyphens, and underscores. The maximum name length is 30 characters.

4 To prohibit call transfers between trunk lines, select *Restricted* (the default value) from the *Trunk to Trunk* drop-down list. Otherwise, select *Unrestricted*.

CAUTION: *If you select* Unrestricted*, telephone users can transfer incoming calls to outgoing trunks. 3Com does not recommend this setting because it enables the possibility of toll fraud.*

5 For T1 Digital Line Cards, modify the Wink Wait value:

- **a** Select Wink Wait from the Timer Values list.
- **b** Type 3000 in the New Value field.
- **c** Click *Apply*.
- **d** Ask your telephone service provider to set their Wink Wait value to 3000 msec.

6 For T1 Digital Line Cards, modify the Guard value:

- **a** Select Guard from the Timer Values list.
- **b** Type 2200 in the New Value field.
- **c** Click *Apply*.
- **d** Ask your telephone service provider to set their Guard value to 2200 msec.

7 Enable the *On Line* check box.

8 Verify that *500* (the default) is in each of the four *AutoExt* fields.

9 Click *OK*.

Verifying Group Membership

To verify that all channels are in the member list:

1 Click the appropriate link:

- *PSTN Gateway Configuration > IT1 Groups*
- *PSTN Gateway Configuration > ISDN PRI Groups*

- *PSTN Gateway Configuration > ISDN BRI Groups*

2 Click the name of a group.

3 Click the Membership tab.

4 Verify that all channels are present.

Completing the Configuration

To complete the Digital Line Card installation:

1 Click the appropriate link:

- *PSTN Gateway Configuration > T1 Channels*
- *PSTN Gateway Configuration > ISDN PRI Channels*
- *PSTN Gateway Configuration > ISDN BRI Channels*

2 Wait approximately 30 seconds for the status of each channel to change from *Ready* to *Idle*.

3 Verify the status of each channel.

If the channel status does not display as Idle*, verify that you have enabled the On Line check box for the card, the span, and the group.*

While you are waiting, you can click Apply *to refresh the list of channels and to see the updated status. If you have connected the telephone company's line to the Digital Line Card, the* Nominal *(on* 3C10165C E1 and *3C10116C T1 Digital Line Cards) or the* CO *(on* 3C10165D E1 and *3C10116D* T1 *Digital Line Cards) status light on the front panel of the Digital Line Card illuminates (solid green). If the light does not illuminate and you have an E1 or T1 line connected, disconnect the line and connect a loopback connector. If the light now illuminates, contact the telephone company for assistance with the line. If the light does not illuminate, contact your 3Com Technical Support representative.*

Digital Line Card Status Lights

This section describes:

- BRI-ST Card Status Lights
- E1 and T1 Digital Line Card Status Lights

BRI-ST Card Status Lights

Each of the four spans on a BRI-ST card has status lights that indicate the status of the span (Table 36).

Table 36 BRI-ST Card Status Lights

Status	D	B1	B2
Off	No Layer 1 connection is established with the Central Office (CO).	The channel is not carrying a call.	The channel is not carrying a call.
Yellow	A Layer 1 connection is established but the channel is not yet ready to make or receive calls.	A call build-up is occurring.	A call build-up is occurring.
Green	The channel is ready to make and receive calls.	A call is connected.	A call is connected.

E1 and T1 Digital Line Card Status Lights

The 3C10165, 3C10165B, and 3C10165C E1 cards and the 3C10116C T1 card display these status lights:

- **CF** — Carrier Fail (when lit, indicates either a red alarm or blue alarm)
- **RA** — Remote Alarm (yellow alarm)
- **LB** — Loopback (when lit, indicates that the card is in loop-back testing mode; does not indicate any of the red, blue, or yellow alarms)
- **Nominal** — The card is framed

The 3C10165D E1 and the 3C10116D T1 cards display these status lights:

- **CO** — Central Office:

  Amber — Alarm condition at the remote end or the CO is not connected or available.

  Green — No alarm condition; the card has a valid connection to the Central Office.

- **POST** — Power On Self Test:

  Off — POST test is running. The test runs approximately 5-seconds after you apply power to the board. After 5-seconds, Off indicates the POST test failed.

  Green — POST test completed successfully.

- **DCH** — D channel status of an ISDN PRI connection:

  Off — No line is attached or the card does not need a D channel, such as when the card is running T1-robbed-bit (CAS).

  Green — Card is configured for ISDN PRI operation and an active PRI connection has been established.

Amber — The D channel has not yet been established. It can take several seconds after the card has completed its power up tests for the card to establish a connection with the PRI trunk. If the DCH light changes to amber after the connection has been established, an active control channel connection through the PRI line might have been lost.

- **DNLD** — Download:

  Flash — The card is downloading software from the Call Processor.

  Green — The download has been completed.

  Amber — The download was interrupted before it completed.

  On a LAN, the download process completes quickly. If the download from Call Processor to Digital Line Card must travel a routed network path, the download might take a few minutes. If the DNLD light remains amber, it might indicate a severely congested network or a hardware problem with the card.

- **CALL** — Call audio traffic:

  Off — No audio traffic on the link.

  Flashing — Audio traffic is present.

- **CARD** — Card Software Status:

  Green — The card has finished downloading software from the Call Processor and all software processes have started successfully.

  Amber — A problem with one or more of the software processes running on the card. The card automatically reboots itself if it detects a problem with any of its software processes.

- **DSP** — Reserved for future use.

- **NCP** — Call Processor communications status:

  Amber — The card is trying to establish contact with a Call Processor.

  Green — The card has established contact with a Call Processor.

- **LNK** — Ethernet link status:

  Green — The 10/100 Uplink port is connected to a 10Mb or to a 10/100 Mb hub or switch.

  Red — The 10/100 Uplink port is connected to a 100 Mb hub or switch.

  Off — There is no connection to the 10/100 Uplink port.

- **ACT**— Ethernet activity

Rapid blink — Data is passing into or out of the card through the 10/100 Uplink port.

Modifying a Digital Line Card

These sections tell you how to modify a Digital Line Card that is already installed in the system:

- Modifying a Span
- Configuring Partial E1 and T1 Lines
- Modifying Span Audio Controls

Modifying a Span

To modify a span:

1. Click the appropriate link:
   - *PSTN Gateway Configuration > T1 Spans*
   - *PSTN Gateway Configuration > ISDN PRI Spans*
   - *PSTN Gateway Configuration > ISDN BRI Spans*
2. Click the MAC address of a span you want to modify.
3. Make the necessary changes. See the online Help for more information about the fields.

Depending on the configuration of the Digital Line Card:

- *The ISDN BRI-ST Digital Line Card supports two or four channels per span.*
- *The E1 Digital Line Card supports 30 channels per span.*
- *The T1 Digital Line Card configured for DS1 supports 24 channels. The T1 Digital Line Card configured for ISDN PRI, it supports 23 channels.*

4. Enable the *On Line* check box to bring the span online.

   Note that the span does not come online unless the card is online first.
5. Click *OK*.

Configuring Partial E1 and T1 Lines

Some telephone companies offer an E1 or T1 line that has less than the maximum number of channels implemented. This is called a *Fractional, Partial,* or *Subequipped E1* and *Subequipped T1*.

Example: To reduce near-term costs, you might decide to purchase 15 channels now and implement more later.

Some telephone companies offer Partial E1and T1 lines as their standard offering, and provide fully implemented E1 and T1 lines only if you make a specific request. If you are unaware of this policy, outbound calls using the E1 or T1 line might fail because, by default, the system places outbound calls using high numbered channels first, and a Fractional E1 or T1 typically has the lower numbered channels implemented.

If you see the *REQ_CHANNEL_UNAVAIL* error message in the span Status window under the *Details of last five calls* heading, follow these steps to determine if a Partial E1 or T1 is causing the error:

1. Remove the highest numbered channel from service (set it offline) and retry the outbound call. See Modifying Card Channels on page 180 for information about how to modify a channel
2. Continue to remove channels until an outbound call succeeds.
3. When the first outbound call succeeds, the highest numbered channel still in service represents the number of active (provisioned) channels in the Partial E1 or T1.
4. Create two groups. Put all of the active channels in one group, and all of the inactive channels in the other. Mark the active group *online* and the inactive group *offline*. See Adding or Modifying a Digital Line Card Group on page 177 for more information about creating groups.

Modifying Span Audio Controls

Normally, you do not need to change the Audio Controls from their default settings. If you have a problem with sound quality that you cannot resolve by using the volume controls on the 3Com telephones, contact your 3Com Technical Support representative.

CAUTION: *Do not change your Audio Controls settings unless a qualified technical support representative instructs you to do so.*

Audio Controls settings affect individual spans. You can edit these properties:

- Silence Suppression (3C10165D cards only) — Enables you to override the system-wide setting. For a detailed description of how silence suppression affects audio quality and bandwidth, see "Audio Settings" on page 37.
- Audio Compression (3C10165D cards only) — Enables you to override the system-wide setting. For a detailed description of how audio

compression affects audio quality and bandwidth, see "Audio Settings" on page 37.

- Audio Source Gain — Enables you to adjust the audio gain to resolve volume issues.

CAUTION: *Do not change your Audio Source Gain settings unless you are instructed to do so by a technical support representative.*

To modify span audio controls:

1. Click the appropriate link:
   - *PSTN Gateway Configuration > IT1 Spans*
   - *PSTN Gateway Configuration > ISDN PRI Spans*
   - *PSTN Gateway Configuration > ISDN BRI Spans*
2. Click the MAC address of the span you want to modify.

   The number of channels supported per span depends on the configuration of the Digital Line Card. E1 cards support 30 channels per span.
3. Click the Audio Controls tab and see the online Help for more information.
4. Enable the *Echo Canceller Enabled* check box if you want to turn on echo cancellation.

   There are two situations in which it might be desirable to disable echo cancellation on a T1 Digital Line Card:
   - If a system is connected to a telephone carrier (Central Office) by a T1 Digital Line Card, and the telephone carrier guarantees to provide echo cancellation on all channels at all times.
   - If T1 Digital Line Cards directly connect two systems, and the network between the two is completely composed of digital circuitry, thus eliminating sources of echo.

   You can enable or disable echo cancellation for each T1 Digital Line Card. However, you cannot enable or disable echo cancellation on individual channels.

CAUTION: *Before you enable echo cancellation for a T1 Digital Line Card, verify that the card is configured for DS1 operation and not ISDN PRI operation.*

5. Click *OK*.

Support of AT&T's 4ESS Switch Protocol

4ESS is the AT&T proprietary version of ISDN. You can select the 4ESS protocol when you configure a T1 Digital Line Card for PRI (Primary Rate Interface) operation. If you select the 4ESS protocol, you can optionally use Call By Call Service Configuration which enables you to select one of three access services:

- SDN (Software Defined Network) — A premises-to-premises service with voice and voice-grade data transport, plus a number of customer-controllable call management and call monitoring features (for example, Virtual Private Networking). You cannot configure SDN as the default setting but you can configure the system dial plan to use SDN.
- MEGACOM — A high-volume outward calling service. MEGACOM can be the default setting.
- Long Distance — The default service if you select the 4ESS protocol, but purchases no other services. You can use Long Distance with SDN but not with MEGACOM.

Selecting the 4ESS Protocol

To enable the 4ESS protocol:

1. Click *PSTN Gateway Configuration* > *ISDN PRI Spans*.
2. Click the MAC address of the desired span.
3. From the *CO Switch Protocol* drop-down list, select *AT&T Custom - 4ESS*.
4. Click either:
   a. *OK* to enable the 4ESS protocol and exit from the window.
   b. *Apply* to enable 4ESS, to remain in the Modify window and configure Call-By-Call Service. See "Setting Up a Digital Line Card at a Remote Location" on page 183 for more information.

Configuring Call-By-Call Service

You order the optional Call-By-Call Service from your long-distance carrier only if you order the 4ESS protocol. 3Com does not support Call-By-Call Service with any other protocol.

To configure Call-By-Call Service:

1. Click *PSTN Gateway Configuration* > *ISDN PRI Spans*.
2. Click the MAC address of the desired span.
3. Enable the *Enable Call-By-Call Service* check box.

4 In the *Carrier Identification Code* field, type the identification code for your long-distance carrier.

Your long-distance carrier can supply this code when you order PRI services, or you can ask the carrier for their code number. Another way to obtain the code is to access the web site for the North American Number Plan Administration (http://www.nanpa.com). In the menu in the left frame, click Numbering Resources > Carrier Identification Codes (CIC). *Click the appropriate links to view the Feature Group B CIC and Feature Group D CIC assignments. Search the documents to determine the identification code for your long-distance carrier. For example, AT&T is listed next to code 288 in the Group D document.*

5 From the *Default Outbound Service* drop-down list, select either *MEGACOM* or *Standard (LDS)* as the service to use as the default. You can configure the system dial plan to use a particular service.

Select MEGACOM as the default service only if you purchased MEGACOM from your long-distance carrier. You cannot select Standard (LDS) as the default service if you purchased MEGACOM, because these two services do not work together.

6 Click *OK*.

Adding or Modifying a Digital Line Card Group

A Digital Line Card group is one or more channels that are assigned the same characteristics, such as Channel Protocol.

These sections tell you how to perform these tasks:

- Adding a Digital Line Card Group
- Modifying a Digital Line Card Group
- Changing Digital Line Card Group Membership
- Removing a Digital Line Card Group

Adding a Digital Line Card Group

You add a new group when you need to assign common characteristics to several Digital Line Card channels.

To add a Digital Line Card group:

1 Click the appropriate link:

- *PSTN Gateway Configuration > T1 Groups*
- *PSTN Gateway Configuration > ISDN PRI Groups*

- *PSTN Gateway Configuration > ISDN BRI Groups*

2 Click *Add* and see the online Help for more information.

Modifying a Digital Line Card Group

You might want to modify a Digital Line Card group to change its name, Auto Extension assignments, or other parameters. When you modify a group, the changes affect all of the Digital Line Cards that are assigned to the group.

CAUTION: *When you modify a Digital Line Card group, you disconnect any active calls on any channels that are associated with the group.*

To modify a Digital Line Card group:

1 Click the appropriate link:

- *PSTN Gateway Configuration > T1 Groups*
- *PSTN Gateway Configuration > ISDN PRI Groups*
- *PSTN Gateway Configuration > ISDN BRI Groups*

2 Click the name of the group that you want to modify.

3 To modify the name of the group, enter a new name in the *Group Name* field. You can use alphanumeric characters, hyphens, and underscores. The maximum name length is 30 characters.

4 Make the necessary changes to the group parameters. See the online Help for more information.

5 Enable the *On Line* check box to bring the group on line.

The group does not come online unless the card and the span are online

6 Click *OK*.

Changing Digital Line Card Group Membership

You might want to modify the channel membership in a group to accommodate changing needs.

Each channel must belong to a group. A channel can belong to only one group. You cannot move a channel from the members list to the non-members list of a group unless the system can assign the channel to another group. If a channel has never been a member of a group, the system cannot determine a group to which it can move the channel. Therefore, it cannot remove the channel from the member list. If a

channel has been a member of a group in the past, the system moves the channel to the group of which the channel was most recently a member.

Example: By default, the system creates two groups, Group 1 and Group 2, and places all channels in Group 1. If you try to move a channel to the non-member list of Group 1, the operation fails. If you:

1. Select Group 2.
2. Click the Membership tab.
3. Move a channel from the non-member list to the member list.
4. Move the same channel back to the non-member list

the operation succeeds because the channel was previously a member of Group 1. If you then view the Group 1 membership list, it contains the channel you just removed from Group 2.

To change group membership:

1. Click the appropriate link:
   - *PSTN Gateway Configuration > T1 Groups*
   - *PSTN Gateway Configuration > ISDN PRI Groups*
   - *PSTN Gateway Configuration > ISDN BRI Groups*
2. Click the name of the group that you want to modify.
3. Click the Membership tab.
4. Enable the *Copy Group Settings to Channels* check box so that the system copies the settings of the group to each channel you add or remove. Otherwise, the system does not change the channel settings.
5. Enable the *Refresh Channels on Add/Remove* field so that the system updates the channel status when you add or remove channels.
6. To add a group member:
   a. If the group does not include any members, enable the check boxes next the MAC addresses that you want to add to the group.
   b. If the I group already has members, click *Show all* to display a list of MAC addresses that you can add to the group's membership.

***Note**: You can toggle between the* Show all *and* Show members only *buttons to display MAC addresses that have membership in the group and the MAC addresses that are not members of the group but who you can add to the group, and to confirm your changes.*

To remove a channel from a group:

1 Clear the check boxes next the MAC address of the channel or channels that you want to remove.

2 Click *OK*.

Removing a Digital Line Card Group

You might want to remove any group that you no longer need.

To remove a group:

1 Click the appropriate link:

- *PSTN Gateway Configuration > T1 Groups*
- *PSTN Gateway Configuration > ISDN PRI Groups*
- *PSTN Gateway Configuration > ISDN BRI Groups*

2 Select the group, or groups, that you want to delete and click *Remove Selected*. To select all groups, enable the *Select* check box.

3 Click *OK* when the system prompts you to confirm.

Modifying Card Channels

The number of channels per span varies according to the configuration. Each channel can accommodate a single telephone call.

This section describes how to modify channels for an installed card and how to view the status of an existing channel.

If you use Auto Discovery to add channels on an E1 PRI line, note that the 30 channels the system discovers are numbered 1 through 15, and 17 through 31. This reflects the physical channel mapping on the E1 interface, in which channel 16 is the ISDN D-channel, that is used for signaling.

CAUTION: *Do not modify channels unless a 3Com Technical Support representative advises you to do so. When you modify an ISDN channel, you disconnect any existing calls on that channel.*

Modifying a Digital Line Card Channel

To modify a channel on an installed Digital Line Card:

1 Click the appropriate link:

- *PSTN Gateway Configuration > T1 Channels*

- *PSTN Gateway Configuration > ISDN PRI Channels*
- *PSTN Gateway Configuration > ISDN BRI Channels*

2 Click the extension of the channel that you want to modify.

3 Complete or change the fields, as necessary. See the online Help for more information.

4 Enable the *On Line* check box to bring the channel on line.

The channel does not come online unless the card and the span are online.

5 Click *OK*.

Viewing the Status of a Digital Line Card Channel

To view the status of an installed Digital Line Card:

1 Click the appropriate link:

- *PSTN Gateway Configuration > T1 Channels*
- *PSTN Gateway Configuration > ISDN PRI Channels*
- *PSTN Gateway Configuration > ISDN BRI Channels*

2 Click the extension of the channel for which you want status information.

3 Click the Status tab.

4 From the Dialog Refresh drop-down list, select:

- Manual — To refresh the *Status* window each time you click *Refresh Device*.
- A time interval (5, 10, 15, 30, or 60 seconds) — to refresh the *Status* window at the specified intervals automatically.

5 Click *Apply,* and then click *OK*.

Viewing DSP (Digital Signal Processor) Details

To view DSP details:

1 Click *PSTN Gateway Configuration > Digital Line Cards.*

2 Click the MAC address of a Digital Line Card.

3 Click the Status tab.

4 In the *DSP List*, click a DSP ID to display the DSP Status window.

5 Click *Close* to close the *DSP Status* window.

Modifying IP Settings

You can modify the IP settings for a Digital Line Card to meet changing requirements.

To use the NBX NetSet utility to modify IP settings, the line card must be on the same subnetwork as the Call Processor.

The BRI and ATC/ALC daughter cards on the 3C10164D-ST card share the same IP address. (There are no individual IP settings for channels on the 3C10164D-ST card, as they all share the same IP address.) Therefore, depending on the configuration, you can change the IP address either of these methods:

- *Click* PSTN Gateway Configuration > Digital Line Cards*, click an extension, and then click the IP Settings tab.*
- *Click* Telephone Configuration > ATA*, click an extension, and then click the IP Settings tab.*

If you change the IP address for any of the daughter cards, the IP address of the other daughter cards changes as well. You can use this method only when the Call Processor and the 3C10164D-ST are located on the same subnetwork.

3C10165D E1 and 3C10116D T1 Digital Line Cards do not support DHCP lease times of less than 20 minutes.

To modify the IP settings of a Digital Line Card:

1. Click *PSTN Gateway Configuration > Digital Line Cards.*
2. Click the MAC address of a Digital Line Card.
3. Click the *IP Settings* tab.
4. To assign IP addresses, enter the first address in the *First IP Address* field. The system sequentially adds the remaining addresses. 3C10165D E1, 3C10116D T1, and 3C10164D BRI Digital Line Cards need only one IP address.

Assigning IP Addresses One at a Time

To assign IP addresses one at a time per channel on cards that support this feature:

1. Click *PSTN Gateway Configuration > Digital Line Cards.*
2. Click the MAC address of a Digital Line Card.
3. Click the *IP Settings* tab.

4 Click *Assign Addresses Individually*.

3C10165D E1, 3C10116D T1, and 3C10164D BRI Digital Line Cards need only one IP address, therefore the *Assign Addresses Individually* button is not present for these cards.

5 Enter the appropriate IP addresses for the channels.

6 Enter IP values in the *Common Subnet Mask* and C*ommon Default Gateway* fields.

7 Click *OK*.

Removing a Digital Line Card

You can remove a Digital Line Card at any time.

CAUTION: *Removing a Digital Line Card might affect your dial plan.*

To remove a Digital Line Card:

1 Click *PSTN Gateway Configuration* > *Digital Line Cards.*

The T1/ISDN Board List shows the installed T1, ISDN PRI, and ISDN BRI cards.

2 Select the card, or cards, that you want to delete and click *Remove Selected*. To select all extensions, enable the *Select* check box.

3 Click *OK* when the system prompts you to confirm.

Setting Up a Digital Line Card at a Remote Location

Each 3C10116D T1, 3C10165D E1, or 3C10164D BRI Digital Line Card can function as a standalone unit and communicate with the Call Processor over a routed network.

To function as a remote card, the card must have the normal IP settings (IP address, default gateway, and subnet mask), plus the IP address of the Call Processor.

The 3C10116D, 3C10165D, and 3C10164D Digital Line Cards can use static IP configuration or they can get their IP configuration from a DHCP server. Auto Discovery downloads the Call Processor IP address to the card. The card stores that information in its non-volatile memory.

3C10165D E1 and 3C10116D T1 Digital Line Cards do not support DHCP lease times of less than 20 minutes.

To configure a Digital Line Card for remote operation:

1. Be sure your system is set for either Standard IP or IP On-the-Fly operation (Click *System-Wide Settings* > *IP Settings*).
2. Install the Digital Line Card in a chassis. You do not need to power down the chassis when you insert or remove cards.

   To identify the card in the NBX NetSet utility, make a note of the card's MAC address printed on the component side of the card.
3. Enable Auto Discovery:
   a. Login to the NBX NetSet utility using the administrator login ID and password.
   b. Click *System-Wide Settings* > *Auto Discovery*.
   c. Enable the *Auto Discover Other Devices (including ATA, Digital Line Cards & Analog Line Cards)* check box, and then click *Apply*.

      When you insert the card, it begins an initialization sequence. Once the power up tests complete, the card communicates with the Call Processor, which begins to update its database. Allow at least 3 minutes for both of these processes to complete. When the card finishes its startup tests and establishes contact with its Call Processor, the Call Processor status light on the card's front panel turns green. You can then disable the *Auto Discover Other Devices (including ATA, Digital Line Cards & Analog Line Cards)* check box.
4. Click *PSTN Gateway Configuration* > *Digital Line Cards* to display a list of available Digital Line Cards in the T1/ISDN Board List.
5. Click the MAC address of the card you just installed and then click the IP Settings tab.

Unlike legacy Digital Line Cards, the 3C10165D E1, 3C10116D T1, and 3C10164D BRI Digital Line Cards use one IP address for all channels on the card.

6. In the *Manually Assigned IP Settings* section, see the *First IP Address*, *Common Subnet Mask*, and *Common Default Gateway* fields.

   If you are using a static IP address for the card:

   a. Type the card's IP address in the *First IP Address* field. The address must be appropriate for the remote network where the card will eventually reside.
   b. Type the subnet mask and default gateway values that are appropriate for the remote network where the card will eventually reside.

c Click *OK*.

The card will restart and go through its startup process. After the card finishes its reboot process, proceed to step 7.

If the remote network where the card will eventually reside uses DHCP to assign addresses:

a If the First IP Address, Common Subnet Mask, or Common Default Gateway fields have an IP address, change each field to 0.0.0.0, and then click *Apply*. After the card finishes its reboot process, proceed to step 7.

b If the First IP Address, Common Subnet Mask, and Common Default Gateway all show 0.0.0.0, assign an arbitrary IP address to any field, and then click *Apply*. The card will restart and go through its startup process again.

c When the card finishes its startup process, refresh the card's IP Settings window. You will see the arbitrary IP address that you assigned.

d Change each field to 0.0.0.0, and then click *Apply*. The card will restart and go through its startup process again.

7 When the card finishes its startup process, it is set with the IP address of its Call Processor. You can now move the card to its remote location where it will use its saved Call Processor IP address to communicate with the system.

Setting Up T1/E1 Logging

The 3C10116D T1 and 3C10165D E1 Digital Line Cards can generate logging information. The system disk drive stores the TEP (**T**1, **E**1, **P**rimary Rate Interface) logs. Use the NBX NetSet utility to view, download, and delete log files. Each card has a separate log, up to a maximum of five log files. When a log reaches its maximum size of 5 MB, it begins to overwrite the oldest data.

Because TEP logging has a performance cost, it is disabled by default. To enable TEP logging and to receive help interpreting the log results, contact your 3Com NBX Voice-Authorized Partner.

Viewing CSU State Information and Statistics

3C10165D E1, 3C10116D T1, and 3C101064D BRI cards have an onboard channel service unit (CSU). Use the NBX NetSet utility to view near end (local CSU) and far end (central office) state information and statistics about each connected span.

To view CSU statistics:

1. Click the appropriate link:
   - *PSTN Gateway Configuration > T1 Spans*
   - *PSTN Gateway Configuration > ISDN PRI Spans*
   - *PSTN Gateway Configuration > ISDN BRI Spans*
2. Click the MAC address of the span.
3. Click the Performance Data tab.
4. Click the appropriate button to choose the type and format the performance data:
   - The system reports the T1 state information and statistics in two formats - T1.231 format and AT&T TR54016 format. Both formats report the same information but they use different terminology.
   - The system reports E1 state information and statistics in a single format - ITU G.826.
   - The system reports G.826 near-end information about the 3C101064D BRI card.

   The system samples performance statistics every 15 minutes and saves up to 24-hours of data in 15-minute intervals. By default, the statistics windows display data from the most recent 15-minute interval. To see other intervals or data from the entire 24-hour period, use the *Select Interval* controls. To display the currently selected data interval in a bar chart, click *Graph*.

   See the online Help for more information about the statistics categories.

T1.231 Near End

To view T1 Span near end statistics in T1.231 format:

1. Log in to the NBX NetSet utility using the administrator username and password.
2. Click *PSTN Gateway Configuration > T1 Spans.*
3. Click a MAC address.
4. Click the Performance Data tab.
5. Click *T.231 Near End*.
6. See the online Help for details for more information.

T1.231 Far End To view T1 Span far end statistics in T1.231 format:

1. Log in to the NBX NetSet utility using the administrator username and password.
2. Click *PSTN Gateway Configuration > T1 Spans.*
3. Click a MAC address.
4. Click the Performance Data tab.
5. Click *T.231 Far End*.
6. See the online Help for details for more information.

TR54016 Near End To view T1 Span near end statistics in TR54016 format:

1. Log in to the NBX NetSet utility using the administrator username and password.
2. Click *PSTN Gateway Configuration > T1 Spans.*
3. Click a MAC address.
4. Click the Performance Data tab.
5. Click *TR54016 Near End*.
6. See the online Help for details for more information.

TR54016 Far-End To view T1 Span far end statistics in TR54016 format:

1. Log in to the NBX NetSet utility using the administrator username and password.
2. Click *PSTN Gateway Configuration > T1 Spans.*
3. Click a MAC address.
4. Click the Performance Data tab.
5. Click *TR54016 Far End*.
6. See the online Help for details for more information.

G.826 Near End To view E1 Span near end statistics:

1. Log in to the NBX NetSet utility using the administrator username and password.
2. Click *PSTN Gateway Configuration > ISDN PRI Spans.*
3. Click a MAC address.

4 Click the Performance Data tab.

5 Click *G.826 Near End*.

6 See the online Help for details for more information.

G.826 Far End To view E1 Span far end statistics:

1 Log in to the NBX NetSet utility using the administrator username and password.

2 Click *PSTN Gateway Configuration > ISDN PRI Spans.*

3 Click a MAC address.

4 Click the Performance Data tab.

5 Click *G.826 Far End*.

6 See the online Help for details for more information.

Using Loopback Tests

The 3C10116D T1 and 3C10165D E1 cards can respond to commands from the Central Office to loop back data at different points for diagnostic purposes.

You use the NBX NetSet utility to *enable* each loopback test and to *initiate* the Local and Framer loopback tests. The Central Office, or test equipment that emulates Central Office equipment, must initiate Line and Payload loopback tests.

For detailed logging information, you can enable TEP logging before you enable loopback testing. However, to set up logging and interpret the logs are advanced tasks that require help from a technical support technician. You can see a simple pass/fail result by viewing the span status, as described in "Enabling or Disabling Loopback Tests" on page 189. To see the loopback test status of all spans, click *PSTN Gateway Configuration > Digital Line Cards > Config & Status Report*.

The cards loop back data at the following points and with the following characteristics:

- **Line Loopback** — A loopback in which the signal returned toward the source of the loopback command comprises the full 1.544 Mbits/s signal with bit sequence integrity maintained, no change in framing, and no removal of bipolar violations.

- **Local Loopback** — An internal (within the framer) diagnostic loopback in which the signal returned towards the source is framed.
- **Framer Loopback** — An internal (within the framer) loopback that tests the path up to where framing is introduced.
- **Payload Loopback** — A loopback in which the signal returned toward the source of the loopback command comprises the payload of the received signal (with bit sequence integrity retained) and newly generated ESF framing (not necessarily maintaining the integrity of the channel timeslots, frames, or superframes of the received signal). The newly generated ESF data link contains a valid performance report message with a value of one in every LB-labeled bit position for the duration of the loopback indicating the signal is the result of a payload loopback.

Enabling or Disabling Loopback Tests

You can use the NBX NetSet utility to enable or disable loopback test support for 3C10116D T1 and 3C10165D E1 cards. By default, loopback test support is disabled. After you enable loopback test support, you can initiate the Local and Framer tests. The Central Office, or test equipment emulating Central Office equipment, must initiate Line and Payload tests.

CAUTION: *If you enable one or more loopback tests, you will terminate any active calls on all channels of the selected span and make that span unavailable for calls until you disable loopback testing.*

To enable or disable loopback support:

1. Login to the NBX NetSet utility using the administrator login ID and password.
2. Click the appropriate link:
   - *PSTN Gateway Configuration > T1 Spans*
   - *PSTN Gateway Configuration > ISDN PRI Spans*
3. Click the MAC address of a span.
4. Enable or disable the Enable Loopbacks check boxes as required and then click *Apply*.

To view the results of Local and Framer loopback testing Span status

1. Login to the NBX NetSet utility using the administrator login ID and password.
2. Click the appropriate link:

- *PSTN Gateway Configuration > T1 Spans*
- *PSTN Gateway Configuration > ISDN PRI Spans*

3 Select the span and click *Status*.

A red alarm indicates that the test failed. No alarm indicates that the test passed.

Obtaining a Dial Tone from a PBX System

To supply dial tone to your system, you can use:

- A third-party PBX system with a digital (T1,E1, or BRI) interface
- An NBX system, which connects to your system by means of a T1 line

When you establish the links between your NBX system and the PBX or another NBX system, the signalling bits provide the dial tone.

If your NBX system connects to another NBX system, make sure the Digital Line Card types are configured as T1. This method is not supported if the Digital Line Card type is configured as ISDN.

1 Click *PSTN Gateway Configuration > Digital Line Cards.*
2 If the Digital Line Card type is ISDN, click the MAC address of the Digital Line Card line.
3 In the *Card Type* drop-down list, select *T1*.
4 Click *Apply.*

Figure 7 shows the pinout for the NBX T1 or E1 Digital Line Card.

Figure 7 T1 or E1 Connector Pinouts

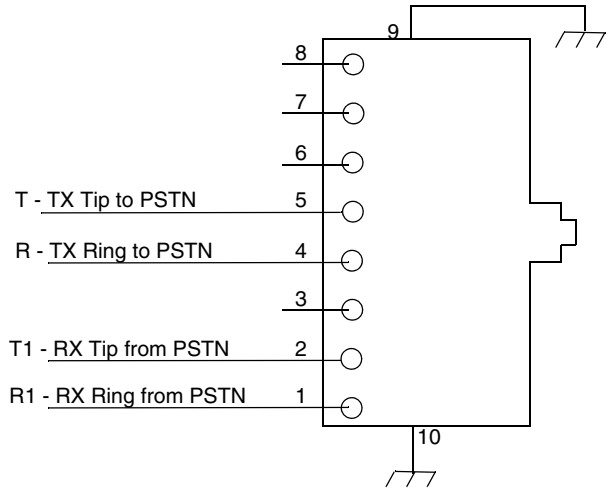
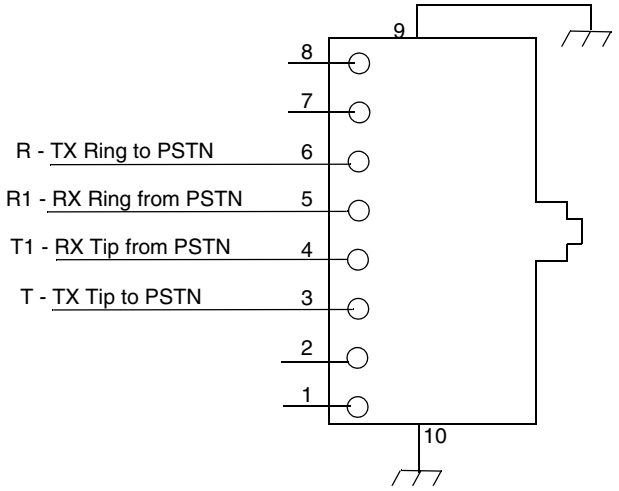


Figure 8 shows the pinout for the NBX BRI Digital Line Card.

Figure 8 BRI Connector Pinouts



To determine the pinout for the PBX T1 or E1 connector, see the PBX documentation.

The transmit pair on the PBX system must connect to the receive pair on the NBX system, and the transmit pair on the NBX system must connect to the receive pair on the PBX system.

To avoid timing issues, either the NBX system or the PBX system must supply the link timing. Typically, the PBX system emulates the Central Office (CO), and the timing mode is set to **Internal** and provides the clock. In this case, set the timing mode of the NBX system to **Loop**.

1. On the NBX system, log in to the NBX NetSet utility using the administrator login ID and password.
2. Click the appropriate link:
   - *PSTN Gateway Configuration > T1 Spans*
   - *PSTN Gateway Configuration > ISDN PRI Spans*
3. Click the appropriate span MAC address.
4. From the *Timing Mod*e drop-down list, select *Loop*.
5. Click *OK*.

If the PBX system only supports Loop timing mode, then set the NBX system timing mode to Internal.

A BRI line operates in TE mode, therefore the CO provides the timing source.

If your configuration includes two NBX systems that are connected by a T1 line, make sure that one system's timing mode is Internal *and the other system's timing mode is* Loop*.*

The PBX system must use a protocol that the NBX system supports. Configure the NBX and PBX systems so that they both use the same protocol.

If your NBX system connects to the PBX system by means of an E1 or BRI line, you must configure the ISDN PRI or ISDN BRI spans.

1. On the NBX system, click the appropriate link:
   - *PSTN Gateway Configuration > ISDN PRI Spans*
   - *PSTN Gateway Configuration > ISDN BRI Spans*
2. Click the appropriate span MAC address.

3. From the *CO Switch Protoco*l drop-down list, select the appropriate protocol.
4. Click *OK*.

If your NBX system connects to the PBX system by means of a T1 line, you must configure the T1 Group settings:

1. On the NBX system, click *PSTN Gateway Configuration > T1 Groups*.
2. Click the appropriate group name.
3. Modify the fields appropriately. See the online Help for more information about the fields.
4. Click *OK*.

9 NBX MESSAGING

This chapter describes how to configure these features of NBX Messaging:

- Group List
- NBX Voice Mail
- Auto Attendant
- Voice Profile for Internet Mail

For more information about these topics and configuration procedures, see the online Help.

If you install a third-party messaging system, the NBX Messaging window is not available in the NBX NetSet utility. Follow the documentation for your voice messaging system.

Group List

System group lists are lists of system users that all telephone users on the system can see and use to send, or append and forward, a voice mail message.

There are 99 System group lists that the system administrator creates and manages. The system identifies System group lists using a two-digit numbering scheme (01 – 99). You can:

- Add System group lists
- Modify System group lists
- Remove System group lists
- List the members of a System group list
- Print a hardcopy of a System group list
- Record a .WAV file of the System group name for identification purposes

The system provides a default System group list that includes all telephone users on the system, and reserves Group ID of 0 for this group. You can later exclude extensions such as conference phones, greeting-only mailboxes, and collective mailboxes (ACD, hunt group, or route point mailboxes) from this default list. Any System group list can include or omit extensions from its list.

A telephone user can include a System group list in a Personal group list, but a System group list cannot contain a Personal group list. For more information about Personal group lists, see NetSet User Help.

NBX Voice Mail

You can configure system-wide settings for telephone users' voice mailboxes (click *NBX Messaging)*. When you add new telephone users to the system, the system creates a mailbox for each user. Telephone users must record a name announcement, a personal greeting, and create a password before they can retrieve their messages.

The system also creates mailboxes for extensions that are not associated with a particular telephone, such as hunt group extension or a TAPI route.

Table 37 describes the fields on the NBX Voice Mail window.

Table 37 Voice Mail Settings

Field	Purpose
Maximum Number of Messages	The number of messages, regardless of length, that an individual mailbox can have. A typical voice message lasts approximately 20 to 30 seconds. **Default:** 30 messages **Maximum:** 512 messages **Minimum:** 1 message

Table 37 Voice Mail Settings (continued)

Field	Purpose
New Message Retention (days)	The maximum number of days that a new (unheard) message remains in a voice mailbox before the system marks it for deletion. However, the message is not deleted until after this sequence of events: ■ The telephone user logs in. ■ The system informs the telephone user that the message will be deleted. ■ The telephone user takes no action to prevent the deletion of the message. ■ The telephone user logs out. **Default:** 30 days **Maximum:** 1826 days (5 years) **Minimum:** 1 day **NOTE:** When a telephone user listens to or saves a new message, the system resets the time stamp for that message. The *Message Retention* value controls when the system marks the message for deletion.
Message Retention (days)	The maximum number of days that a message remains in the mailbox after a telephone user has listened to or saved it. The system then marks the message for deletion. However, the message is not deleted until after this sequence of events: ■ The telephone user logs in. ■ The system informs the telephone user that the message will be deleted. ■ The telephone user takes no action to prevent the deletion of the message. ■ The telephone user logs out. **Default:** 30 days **Maximum:** 1826 days (5 years) **Minimum:** 1 day
Maximum Incoming Message Length (minutes)	The maximum length, in minutes, for any one message. **Default:** 5 minutes **Maximum:** 10 minutes **Minimum:** 1 minute
Voice Mail Compression Format	The system uses ADPCM as the voice mail compression format for voice prompts and messages.

Table 37 Voice Mail Settings (continued)

Field	Purpose
On Disk Voice Mail Format	The system uses ADPCM as the compression format for voice prompts and mail on your disk.
Disable AA Transfer Prompt	Enables or disables the transfer prompt ("*Please hold while your call is transferred*") when the Auto Attendant transfers a call. **Default:** Disabled

Additional Considerations

- The maximum length of a voice mail message is 10 minutes. If accumulated messages fill the system's message storage space before individual telephone users reach their capacity limits, either lower the mailbox settings or upgrade your message storage option. If you decrease mailbox settings, you do not affect data already in storage. You can also encourage telephone users to delete old messages.
- To view your system's current message storage capacity, click *Licensing and Upgrades* > *Licenses*. The system displays the number of NBX Voice Mail/Auto Attendant ports and storage space (in hours on an NBX 100 system). The number of ports determines how many voice mail sessions and Auto Attendants can be in use simultaneously.
- Each voice mail extension enables one voice message session. If all voice mail extensions are in use, call behavior differs depending on the operation. If the Attendant Console forwards calls to the Auto Attendant, and all voice mail extensions are in use, an outside caller hears ringing but no answer until an extension is free. If an internal telephone user transfers a caller to voice mail, but no voice mail extensions are available, the call rings back to the caller's extension.
- As the system administrator, you can configure voice mail extensions, settings, passwords, and off-site notification. the NBX NetSet utility also reports on the status and usage of voice mail ports and voice mail storage usage by telephone user. For details, see these sections:
  - Voice Mail Extensions
  - Voice Mail Passwords
  - IMAP for Integrated Voice Mail
  - Off-site Notification
  - Status
  - Port Usage

- User Usage

Voice Mail Extensions

The number of voice mail ports on your system determines the number of voice mail sessions that can take place at one time. The default system includes 4 voice mail ports. You can purchase a license for additional capacity. Each voice mail port has an extension number. See "Extension Settings Overview" on page 282 for more information.

Voice Mail Passwords

To retrieve voice messages, a telephone user must log on using the extension number and password. The password, a 4-digit to 10-digit number, allows access to Personal Settings in the NBX NetSet utility and to voice mail from the telephone. The telephone user can change the password from the telephone or by logging in to the NBX NetSet utility

The administrator can reset a user password to the user's extension number. See "Password Administration" on page 80 for information about Security features.

For more information about the menus and features available to telephone users, see the *NBX Telephone Guide* and the NBX NetSet utility User Help.

IMAP for Integrated Voice Mail

NBX Voice Mail uses an Internet Message Access Protocol (IMAP) server, which enables telephone users to access and manage their voice messages through any IMAP-compliant e-mail client. As the system administrator, you might need to help telephone users to configure e-mail clients.

Voice mail messages can be sent as mail messages with.WAV file attachments. You double-click an attachment to activate the computer's media player, and the voice message plays through the speakers or earphones on your computer. After you listen to a message, it loses its "new" status, but it remains on the server until you delete it using the IMAP e-mail client, the telephone, or the Personal Settings window in the NBX NetSet utility, or until the system deletes it when it is older than the system limit (after a warning message). The computer used to receive messages must support multimedia.

You cannot compose new voice mail messages through your IMAP e-mail client. You must use your telephone.

To process both e-mail and voice mail on one computer, you need either of the following:

- An e-mail client that can connect to two servers
- Two instances of the e-mail client

Setting Up an e-mail Client to Access Messages

Because each e-mail client has a unique configuration interface, the following procedure is presented in general terms only. See your e-mail client's documentation to determine how to accomplish a specific task.

1. Determine if the e-mail client can communicate with an IMAP 4 server.

   Some versions of Microsoft Outlook and Outlook Express, Netscape, and Eudora support IMAP. Check your e-mail program's documentation to determine if it supports IMAP.

2. Set the *Incoming Mail Server* to the IP address or to the host name of your system.

   Set the *Outgoing Mail Server* to the mail server in use for regular e-mail.

   The NBX IMAP server cannot perform address translation, so you cannot use the system as your company e-mail server.

3. If necessary, identify the server type as *IMAP*.
4. For the username, specify the user's telephone extension number. For the password, specify the user's voice mail password.

Configurable Operators

You can allow callers to forward their call to one of two configurable operators when they reach a telephone user's voice mailbox. You or the telephone user can choose how to manage calls. The configurable operators are:

- **System Operator** — This is the standard System Operator for your site.
- **Personal Operator** — This is a destination other than the default System Operator that would be appropriate for a call placed to you. For example, a Personal Operator might be your executive assistant, your cell phone, or a hunt group.

If you do not wish to employ configurable operators, the default System Operator (extension 501) remains in place.

The caller presses a number (the **access digit**) on the key pad to reach either operator. The access digit for the System Operator is either **0** or **9**; the access digit for the Personal Operator is the digit you did not use for the System Operator. (Access digits cannot be the same for both operators.)

The two operators are functionally identical: either can be referenced as the Personal Operator or the System Operator, depending on your site's requirements. For example, you could designate the extension for the System Operator as your Personal Operator.

What Can You Assign As An Operator?

As the system administrator, you can assign any of the following as an operator destination:

- System extension

  A system extension can be Auto Attendant or another extension within your facility.
- Hunt group
- External telephone number
- Virtual Tie Line (VTL) extension

Feature Support For Configurable Operators

The following features and desktop applications support Configurable Operators:

- Call Group mailboxes, hunt group mailboxes, and TAPI route points support the Configurable Operators feature; otherwise, the defaults apply.
- Virtual Tie Lines (VTLs) — Personal operators can accept a VTL extension.
- Phantom Mailboxes — Phantom mailboxes support the Configurable Operators feature. The destination can be either an internal extension, Auto Attendant, or voice mail.
- Greeting-only Mailboxes — Greeting-only Mailboxes support the Configurable Operators feature.

How the Configurable Operator Feature Works

When the system directs a caller from your voice mail to an operator that you designated:

1. If you do not answer a call, the system invokes your voice mail.
2. The caller listens to your pre-recorded voice mail message, which includes the instruction to press an access digit (**0** or **9**) to reach the appropriate operator.

When you employ a configurable operator, you must re-record your personal voice mail greeting to explain to callers that an operator is available to them if they press the appropriate access digit during the voice mail greeting.

3. The caller presses **0** or **9**.
4. The system redirects the call to the operator that you designated.

   The caller can leave a message, then press **0** or **9** to transfer to a configured operator.

Configuring Operator Destinations

To configure system default operator destinations:

1. Log on to NetSet using the administrator login ID and password.
2. Click *NBX Messaging* > *Configure*.
3. Click the *Personal Operator* tab.

   The editable fields display the current system default values for System Operator and Personal Operator.

You cannot leave the system default values for the operators as null. Also, the text string for an operator destination cannot exceed 16 characters.

4. Edit the operator numbers and the access digits as appropriate.
5. Click the *Apply* button to make the changes and keep this window open, or click the *OK* button to make the changes and close the window.

Off-site Notification

Off-site Notification can notify telephone users by pager, e-mail, or telephone when they receive a new voice mail message. Telephone users can specify the methods by which they receive notification.

You can configure these system-wide Off-site Notification settings:

- Enable or disable Off-site Notification for the entire system

- Set the maximum number of out-calling ports
- Assign an out-dialing prefix for Off-site Notification

To configure Off-site Notification, click *NBX Messaging* > *Configure* and click the Off-site Notification tab.

Table 38 provides details on Off-site Notification fields.

Table 38 Off-site Notification Fields

Field	Purpose
Offsite Notification Enabled	Enables Off-site Notification throughout the system. By default, Off-site Notification is disabled. When you enable Off-site Notification, you must also enable it for: ■ Class of Service Settings. See Class of Service (CoS) on page 132. ■ The telephone user's personal settings. See "Off-Site Notification" in the *NBX Telephone Guide*.
Max Out-calling Ports	The number of voice mail ports available for simultaneous use by Off-site Notification. You can configure this parameter for up to the number of voice mail ports licensed for the system. The system is shipped with 4 ports; purchase an upgrade license to enable additional ports.
Out-dialing Prefix	A prefix used by every call made by Off-site Notification. If this setting is empty, the call uses only the information specified by the telephone user.

Notes About Off-site Notification

- To allow telephone users to take advantage of Enable Off-site Notification, you must perform these three steps:
  - *Click NBX Messaging* > *Configure* and click the Off-site Notification tab to enable Off-site Notification system wide.
  - Click *User Configuration* > *Class of Service* and click the CoS Group Name to enable Off-site Notification in the Class of Service settings.
  - Verify that the individual telephone user's extension has been enabled for Off-site Notification.
- Before Off-site Notification can send e-mail, define an SMTP Domain Name, and one or more valid Domain Name Servers (click *System-Wide Settings* > *IP Settings)*.

- When you use Off-site Notification:
  - If you choose *Pager* or *Voice Mail* as the *first* notification method, the system notifies you only of the *first* new message you receive after the time you have most recently logged in to your voice mailbox. The system does not notify you each time you receive a new message. The next time you log on to your voice mailbox, Off-site Notification is re-enabled.
  - If you choose *EMail* as the *first* notification method, you receive a notice for each message. The system attaches the message to the e-mail as a .WAV file. If you configure *any* method in any of the remaining four attempt lines, the system also attempts each specified method for each new voice mail message.
  - If you configure more than one notification attempts, configure them in order. For example, if you configure three attempts, configure them on lines 1 through 3, without unconfigured lines in between.
  - If you disable NBX Messaging in favor of another messaging application, the *Offsite Notification* is unavailable.

Status To view the status of all voice mail ports on this system, click *NBX Messaging* > *Configure* and click the Status tab.

You can also reset a voice mail port. Select the extension, or extensions, that you want to reset and click *Reset*. To select all extensions, enable the *Select* check box.

Table 39 explains the information in the Status window.

Table 39 Fields in the Status Window

Column	Purpose
Extension	The extension that is associated with the voice mail port.
Name	The name that is associated with the voice mail port.

Table 39 Fields in the Status Window (continued)

Column	Purpose
Used By	The person or device that is using the voice mail port. **Values:** ■ Extension number, name — The extension number and name of an internal telephone user that is using the voice mail port. ■ Auto Attendant — The Automated Attendant is using the port. ■ Blank — The port is not being used. The system displays *Idle* in the *In Use* column.
In Use (Seconds)	The length of time, in seconds, that the voice mail port has been in use. If the port is not in use, the system displays *Idle*.
On Hold	Indicates whether the voice mail port is on hold. The system places voice mail ports on hold in the same way that it places a call on hold. **Values**: Yes, No

Port Usage

To determine how busy the system's voice mail ports are, and whether additional ports might be necessary, click *NBX Messaging* > *Configure*, and then click the Port Usage tab. See the online Help for details about the report.

The system displays parameters in the Port Usage report in red to alert you that a problem exists. For example, if "Missed messages caused by full mailboxes" changes to red, you might need to increase the maximum number of messages allowed per mailbox.

User Usage

To determine user impact on the voice mail system, click *NBX Messaging* > *Configure*, and then click the *User Usage* tab.

The User Usage report provides the current number of new and saved voice mail messages for each telephone user and calculates the amount of storage each telephone user's messages consume. This report lists any type of mailbox, including telephone, phantom, TAPI route point, and hunt group mailboxes.

Deleting User Voice Mail

From the User Usage report, you can also delete the voice mail messages for a selected telephone user. Select the extension, or extensions, from

which you want to delete voice mail and click *Delete VM*. To select all extensions, enable the *Select* check box.

The time the system requires to delete a telephone user's voice mail depends on the number of voice mail messages in the user's mailbox.

Auto Attendant

The NBX Messaging system includes an Auto Attendant that answers incoming calls. The Auto Attendant includes a series of recorded messages (prompts) that describe actions that a caller can take to access individual services. You can customize the menu structure and record or import your own prompts to fit the system to your business needs. This section provides information about these topics:

- Overview of Auto Attendant Features
- Adding an Auto Attendant
- Voice Application Setup Utility
- Testing the Auto Attendant

Overview of Auto Attendant Features

The Auto Attendant is the centerpiece of the voice mail system. You can create and configure Auto Attendants, and can record or import messages and prompts to direct the actions of callers.

Use the NBX NetSet utility to administer and configure these Auto Attendant features:

- **Multiple Auto Attendants** — The system supports multiple, independent Auto Attendants. You can assign different Auto Attendants to different extensions, inbound lines or DID numbers. See "Adding an Auto Attendant" on page 208 for more information.
- **Multiple-Level Menus** — Each Auto Attendant can support a main menu and up to 19 levels of submenus. You to configure an automated system in which inbound callers can select specific departments or groups, and then further select subgroups or individuals. See "Prompt Menus" on page 210 for more information.
- **Voice Prompts** — To the caller, the time-dependent greeting, main menu prompt, and submenu prompt are integrated into the Auto Attendant system. You can customize the system by recording or importing voice prompts in a time-dependent greeting main menu, or submenu. Depending on the time of day and selections that the caller

makes, the caller hears the appropriate prompts and receives appropriate directions.

- **Default Time-out** — If a caller does not respond to the Auto Attendant prompts (for example, a caller that uses a rotary telephone), the system routes the call to a designated time-out destination. See "Prompt Menus" on page 210 for more information.

If you do not specify a valid time-out destination for an Auto Attendant, the system drops a call when it reaches the time-out value.

- **Shortcuts** — Callers can press a shortcut button to bypass an entire greeting or prompt and move directly to a function, such as leaving a voice mail message.
- **Dialing by Extension or Name** — A caller can reach a person by dialing the person's extension. The system plays the announcement of each person identified as a possible match and asks the caller to pick one.
- **Dialing by First Name or Last Name** — A caller can reach a person by dialing the person's name on the telephone keypad. After the caller selects the Name Directory option, Auto Attendant prompts the caller to select whether to use the first-name method or last-name method. When the caller begins to enter the name on the keypad, Auto Attendant performs a database lookup and prompts the caller with the possible matches. The caller selects the appropriate name, and Auto Attendant transfers the call to the selected telephone user.
- **Automatic Activation** — The system can activate automatically according to the Business Hours settings (see "Business Hours" on page 35), or after an incoming call exceeds a set number of rings.
- **Routing Calls to Specific Auto Attendants** — You can use the dial plan to map Auto Attendants to specific analog telephone extensions. This enables the system to route incoming calls directly to a specific Auto Attendant.
- **Voice Application Setup Utility** — From the 3Com Business Telephone, you can use the Auto Attendant Voice Application Setup utility to set up these Auto Attendant features:
  - Button actions
  - Time-dependent greetings and schedule
  - Main menu greeting
  - Administrator's Auto Attendant password

For more information, see "Voice Application Setup Utility" on page 221.

Adding an Auto Attendant

The system includes two Auto Attendants: the Default Menu (extension 500), which manages incoming calls, and the VoiceMail Menu (extension 501), for employee access to voice mail. You cannot delete these two Auto Attendants. The default Auto Attendant processes calls as soon as you install the system. When you add a new Auto Attendant, you are add a blank Auto Attendant, which you can configure.

To add a new Auto Attendant, click *NBX Messaging* > *Auto Attendant* > *Add*.

Table 40 describes the fields and checkbox on the *Add Auto Attendant Menu* window.

Table 40 Add Auto Attendant Menu Fields

Field	Purpose
Name	Enter a name for the new Auto Attendant.
Extension	The system automatically assigns the next available extension when you add a new Auto Attendant. You can change the extension number to an unused number that falls within the Auto Attendant extension range of your dial plan. **Default range:** 3-digit dial plan: 500–599 4-digit dial plan: 5500–5599 For both 3-digit and 4-digit dial plans, the default Auto Attendant is extension 500 and the voice mail Attendant is extension 501.
Maximum number of prompt repeats	Select the number of times the Auto Attendant prompt repeats. You can select a number from 1 through 3. The default is 3. **CAUTION:** If you set this field to 1 and the time-out action for the Auto Attendant menu tree to Disabled, the system disconnects a call forwarded to the Auto Attendant because the forwarding party always hears a portion of the Auto Attendant prompt. Likewise, if you set this field to 2 or 3 and the time-out action for the Auto Attendant Menu Tree to Disabled, the system disconnects the forwarded call if the forwarding party stays on the line long enough to hear at least a portion of the final repeated prompt. To ensure that forwarded calls eventually reach a valid destination, configure a time-out action for each Auto Attendant menu tree.

Table 40 Add Auto Attendant Menu Fields (continued)

Field	Purpose
Use System-wide Greetings checkbox	Enable this checkbox so that the system uses all three system-wide greetings (Morning, Afternoon and Evening) by default. To enable or disable individual system-wide greetings for a particular Auto Attendant, click *NBX Messaging* > *Auto Attendant*, click a specific extension, and then click the TD Greetings tab.

After you add or modify an Auto Attendant, you can configure the following features:

- Play/Record Extension
- Time-dependent Greetings
- Prompt Menus
- Auto Attendant Buttons

Play/Record Extension

The *Play/Record Extension* identifies the telephone on which you can work interactively with the NBX NetSet utility to record and listen to Auto Attendant prompts. Typically, this is the extension of the person who configures and administers the Auto Attendant. An Auto Attendant prompt is an audio file (.WAV) that is associated with a specific Auto Attendant. It describes the actions a caller can take.

When you click the button in the NBX NetSet utility to record or play a prompt, the extension rings. When you answer it, you either hear the prompt you selected to play or you are prompted to record a prompt.

You cannot customize any greetings or prompts until you specify this extension.

To specify a play/record extension, click these links:

- *NBX Messaging* > *Auto Attendant.*
- *NBX Messaging* > *Auto Attendant* and then click the System Wide Greetings tab.
- *NBX Messaging* > *Auto Attendant, a specific extension, and then click the Prompt or TD Greetings tab.*

Time-dependent Greetings

The system clock and the greeting schedule control when the system changes from one time-dependent greeting to the next. For example, the morning greeting might start at 12 midnight, the afternoon greeting at noon, and the evening greeting at 6 p.m. If you enable time-dependent greetings, the caller hears the current active greeting before the main menu prompt.

You can create time-dependent greetings for all Auto Attendants in your system. An example of this system-wide greeting might be "Good morning." To record or to import system-wide time-dependent greetings and define the times during which they play, click *NBX Messaging* > *Auto Attendant* and click the System-Wide Greetings tab.

You can also create and schedule time-dependent greetings for individual Auto Attendants. These greetings can be up to five minutes long. To record, import, or schedule customized time-dependent greetings, click *NBX Messaging* > *Auto Attendant,* click a specific Auto Attendant extension and then click the TD Greetings tab.

Prompt Menus

You can use a main menu and submenus of prompts to direct callers to individuals and services in your organization. To configure prompt menus for each Auto Attendant, click *NBX Messaging* > *Auto Attendant,* click a specific extension and then click the Menu Tree tab. The Menu Tree window consists of 13 button rows that you use to assign actions to the key pad buttons (see"Auto Attendant Buttons" on page 215). Be sure to define the menu time-out behavior so that the system automatically routes calls to a time-out destination if a caller does not respond to the Auto Attendant prompts (for example, a caller that uses a rotary telephone).

CAUTION: *To ensure that forwarded calls eventually reach a valid destination, configure a time-out action for each Auto Attendant menu tree. For example, if you set the time-out action for the Auto Attendant menu tree to* Disabled*, and* Maximum number of prompt repeats *to* 1*, the system disconnects a call forwarded to the Auto Attendant because the forwarding party always hears a portion of the Auto Attendant prompt. Likewise, if you set the time-out action for the Auto Attendant Menu Tree to* Disabled*, and* Maximum number of prompt repeats *to* 2 *or* 3*, the system disconnects the forwarded call if the forwarding party stays*

on the line long enough to hear at least a portion of the final repeated prompt.

Main Menus If you enable a time-dependent greeting, the main menu prompt follows it. The main menu prompt describes all Auto Attendant options and can be up to five minutes long. The default Auto Attendant main menu prompt states:

"If you know the extension of the party you want to reach, you may enter it at any time. To reach the name directory, press 9. To reach the Auto Attendant, press 0 or remain on the line. Thank you for calling."

By default, the Auto Attendant main menu provides callers with the functions that Table 41 describes.

Table 41 Auto Attendant Default Configuration

Button	Action
Numbers	These buttons allow callers to dial these user extensions: V3001R, V3000, and V5000 systems: 1000–3999 **NOTE**: These systems are shipped with a factory default 4-digit dial plan. If you import any 3-digit plan, you must manually specify any 3-digit extension ranges that are not set by the imported plan. NBX 100 systems: 100–449 **NOTE**: The NBX 100 system is shipped with a 3-digit dial plan. If you import any 4-digit plan, you must manually specify any 4-digit extension ranges that are not set by the imported plan.
9	Connects to the Name Directory.
0	Transfers to the extension specified in the menu tree for the Auto Attendant, usually the extension of the receptionist's telephone. The default extension is: **V3001R, V3000, and V5000 systems:** 1000 **NBX 100 systems:** 100
*	Prompts the caller for a mailbox number and then transfers the call directly to the specified mailbox.
#	Exits from the system.

Table 41 Auto Attendant Default Configuration (continued)

Button	Action
T/O	A menu time-out action; transfers to the extension specified in the menu tree for the Auto Attendant, usually the extension of the receptionist's telephone. The default extension is: **V3001R, V3000, and V5000 systems:** 1000 **NBX 100 systems:** 100 **NOTE**: Always configure a timeout action for an Auto Attendant top level menu. The system will disconnect a call if the call times out and there is no valid action defined.

To create a main menu, click *NBX Messaging* > *Auto Attendant,* click a specific Auto Attendant extension, and then click the Menu Tree tab. To create or import voice prompts, click *NBX Messaging* > *Auto Attendant,* click a specific Auto Attendant extension, and then click the Prompt tab. See the online Help for procedures to create menus and prompts.

Submenus An Auto Attendant main menu can branch to submenus to keep the main menu brief, and to give the caller a variety of choices. Each submenu has a prompt that informs the caller of the option that each key pad button provides.

If you have a large organization, the caller might have to enter several digits and listen to several submenus before reaching the person or department. For example, the caller might hear:

"To reach our Sales Department, press 1. For Technical Support, press 2..."

The caller selects option 1 for sales and hears:

"For European Sales, press 1. For North American sales, press 2."

The caller requires North American sales, presses 2, and is connected to a sales hunt group.

To configure submenus, click *NBX Messaging* > *Auto Attendant,* click a specific Auto Attendant extension, and then click the Menu Tree tab. See the online Help for procedures to set up submenus.

For an example that uses submenus, see "Three Greetings, a Main Menu, and a Submenu" in the next section.

Examples

These examples illustrate some typical Auto Attendant systems. They illustrate the kind of information that you might include in your time-dependent greetings, main menu prompts, and submenu prompts.

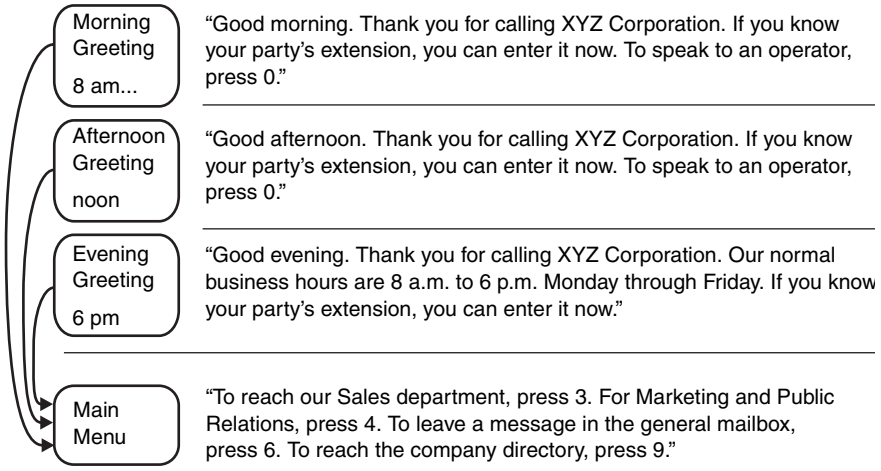
No Greetings Figure 9 shows the simplest configuration. The time-dependent greetings are disabled; the Main Menu contains all of the prompts. In Example 1, callers hear the same message no matter what time they call.

Figure 9 No Time-dependent Greetings, All Prompts in Main Menu

In this example, the main menu is configured to map button 3 to a Sales submenu and button 4 to a Marketing and Public Relations submenu. Button 9 is mapped to the Name Directory.

Three Greetings and a Main Menu Figure 10 shows a simple Auto Attendant that uses time-dependent greetings to provide different messages for different times of the day.

Figure 10 Three Time-dependent Greetings and Main Menu

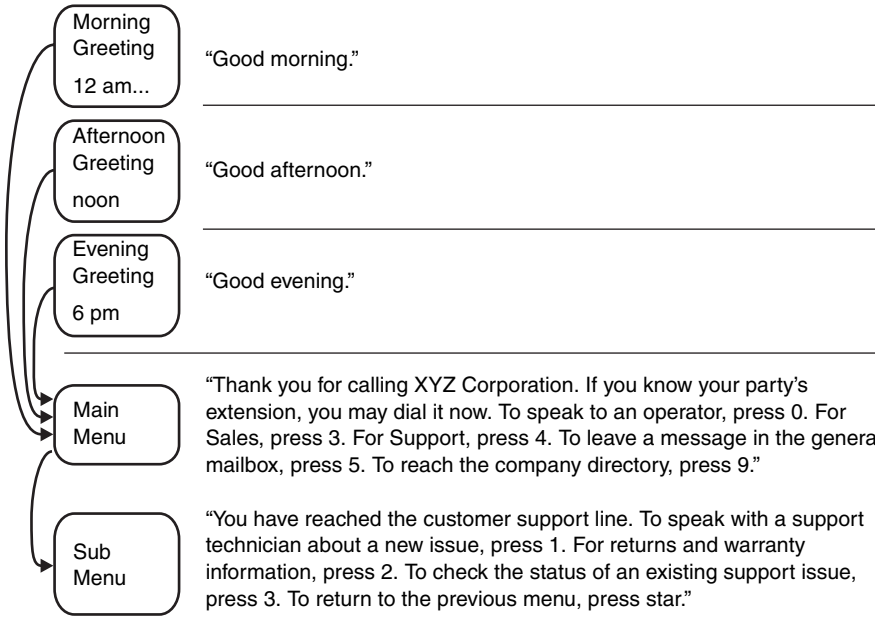


In this example, the morning greeting starts at 8 a.m. and is active until the afternoon greeting begins at noon. The evening greeting begins at 6 p.m.

The function that you allocate to a button on the keypad remains the same throughout the day.

Three Greetings, a Main Menu, and a Submenu Figure 11 shows an example that uses time-dependent greetings, a Main Menu, and a Submenu.

Figure 11 Three Time-dependent Greetings, a Main Menu and a Submenu



This example uses time-dependent greetings to greet callers according to the time of day. The main menu prompt presents callers with options for reaching the operator, specific departments, or the company directory of names. It also uses a submenu to direct callers to subgroups within the Support department.

Auto Attendant Buttons

You can configure the key pad button actions presented to a caller by the Auto Attendant (click *NBX Messaging* > *Auto Attendant,* click a specific Auto Attendant extension, and then click the Menu Tree tab). For examples of how you can use prompts and greetings in an Auto Attendant, see "Examples" on page 213.

Table 42 describes the Menu Tree fields.

Table 42 Menu Tree

Field	Purpose
Button	Lists the buttons on the telephone key pad.

Table 42 Menu Tree (continued)

Field	Purpose
Task Description	Describes the key pad button operation. If you assign the *Enter Submenu* action to the button, this description is used as the Submenu name.
Action	Contains a drop-down list box that lists the actions you can assign to a key pad button. The Auto Attendant prompts callers to press buttons to perform specific actions. You must configure the Menu Tree to so that each button performs the proper action. For a complete list of button actions, see Table 43.
Value	Describes the value associated with each key pad button action. For a complete list of key pad button actions, see Table 43.

You can assign keypad actions to each button on a typical telephone key pad, 0 through 9, #, and *.

Table 43 describes the actions you can assign to buttons. Most systems use no more than five action choices to avoid confusing callers. If you need to present more than five choices, use submenus to configure these additional options. See "Submenus" on page 212.

To create an unannounced option, map a button without creating a corresponding prompt. Callers do not hear a message that the choice is available.

Table 43 Button Actions

Action	Description
Disabled	The system takes no action when the telephone user presses this button. A prompt announces *invalid key*. If assigned as a menu time-out action (T/O), Disabled either leaves the system or goes to a parent menu, depending on where the attendant is in the menu hierarchy. **CAUTION:** If you set this field to 1 and the time-out action for the Auto Attendant menu tree to Disabled, the system disconnects a call forwarded to the Auto Attendant because the forwarding party always hears a portion of the Auto Attendant prompt. Likewise, if you set this field to 2 or 3 and the time-out action for the Auto Attendant Menu Tree to Disabled, the system disconnects the forwarded call if the forwarding party stays on the line long enough to hear at least a portion of the final repeated prompt. To ensure that forwarded calls eventually reach a valid destination, configure a time-out action for each Auto Attendant menu tree. *Value* — Not used.
Name Directory	Allows a caller to spell a person's name on the keypad. The system matches the letters that the caller enters to a Last Name in the list of User Profiles. If the system finds more than three matches, it prompts the caller to enter more letters. When the system narrows the choice to three or fewer, it offers the caller a choice by playing the recorded name greeting of each choice. During a search, the system ignores any User Profile that does not have a recorded greeting. *Value* — Not used.
System Disconnect	Allows the caller to have the system close the connection. This feature can save time for callers who call into the system using a calling card. By having the system disconnect them instead of breaking the connection themselves, callers can make other calls without re-entering all of their calling card information. To activate System Disconnect, the telephone user must press the key defined in the menu and then, when prompted, the key defined in the Value box. Typically, you do not include these instructions in the Auto Attendant prompt, which is heard by all callers. Instead, you make your system users aware of this sequence. *Value* — Any of 0-9, #, *
Transfer to Voice Mail	Allows callers to leave a voice message for a person without ringing that person's phone, or allows telephone users to call in and listen to their voice mail from a remote location. *Value* — Not used.

Table 43 Button Actions (continued)

Action	Description
Exit Menu	Available in submenus only. Allows the caller to return to the next menu up in the menu tree. *Value* — Not used
Prompted Transfer	Instructs the caller to press a button before dialing a known extension. The prompt might state: "If you know your party's extension, press 5, and then dial the extension." *Value* — Not used.
Reserved in Dial Plan	Interprets a specified button as the first number of an extension. For example, in the default 4-digit dial plan, extensions begin at 1000, so you could not use 1 as an option for an Auto Attendant menu. *Value* — Not used
Single Digit Transfer	Allows a caller to press a specific button to reach a specific destination. For example, you might assign button `6` to a hunt group extension in the Sales Department. In the menu prompt, you can record: "`To reach our Sales Department, press 6.`" You can also use Single Digit Transfer to specify a destination, typically the Attendant Console extension, for the time-out option (T/O). By default, Single Digit Transfer can forward calls only to internal extension numbers. To transfer calls to an external number, you must first alter Table 2 of the dial plan (Incoming Table) to specify the external number. *Value* — Any valid extension

CAUTION: Be careful when you use Dial Plan Table 2 to allow access to PSTN ports, which can allow toll fraud.

Table 43 Button Actions (continued)

Action	Description
Enter Submenu	Puts the caller into a submenu of options. When you assign the *Enter Submenu* action to a button and then click *Apply,* the system displays a down-arrow button to the right of the row. Click this down-arrow button to configure the submenu that you want to associate with the main menu. The entry in the *Task Description* field for this button becomes the submenu name. Submenu button actions include "Exit menu" to allow callers to return to the next highest menu. Otherwise, submenu button actions are identical with main menu button actions. Each menu can have up to 20 levels of submenus. For an example that uses submenus, see "Three Greetings, a Main Menu, and a Submenu" on page 214. *Value* — Not used

Activating Changes

After you modify a greeting or prompt (or any Auto Attendant setting), you must activate these changes in the Auto Attendant before they become effective. The **!>** characters next to an Auto Attendant in the Auto Attendant list indicate that you must activate the Auto Attendant.

To activate changes, click *NBX Messaging* > *Auto Attendant,* select a specific Auto Attendant extension, and click *Activate*.

If you do not click Activate*, the system does not implement the changes when you click* Apply*.*

Managing Auto Attendants

This section describes additional ways in which you can manage Auto Attendants.

- Modifying an Auto Attendant
- Removing an Auto Attendant
- Restoring Auto Attendant Greetings

Modifying an Auto Attendant

To modify an Auto Attendant, click *NBX Messaging* > *Auto Attendant* and click a specific Auto Attendant extension.

Table 40 describes the fields and checkbox tin the Modify Auto Attendant Menu window.

Table 44 Modify Auto Attendant Menu Dialog Box

Field	Purpose
Name	Edit the name of the Auto Attendant.
Extension	Edit the extension number by changing it to an unused number that falls within the Auto Attendant extension range of your dial plan. **Default range:** 3-digit dial plan: 500–599 4-digit dial plan: 5500–5599 For both 3-digit and 4-digit dial plans, the default Auto Attendant is extension 500 and the voice mail Attendant is extension 501.
Maximum number of prompt repeats	Edit the number of times the Auto Attendant prompt repeats. You can select a number from 1 through 3. The default is 3.
CAUTION: If you set this field to 1 and the time-out action for the Auto Attendant menu tree to Disabled, the system disconnects a call forwarded to the Auto Attendant because the forwarding party always hears a portion of the Auto Attendant prompt. Likewise, if you set this field to 2 or 3 and the time-out action for the Auto Attendant Menu Tree to Disabled, the system disconnects the forwarded call if the forwarding party stays on the line long enough to hear at least a portion of the final repeated prompt. To ensure that forwarded calls eventually reach a valid destination, configure a time-out action for each Auto Attendant menu tree.	
Use System-wide Greetings	Enable this checkbox so that the system uses all three system-wide greetings (Morning, Afternoon and Evening) by default. To enable or disable individual system-wide greetings for a particular Auto Attendant, click *NBX Messaging* > *Auto Attendant*, click a specific extension, and then click the TD Greetings tab.

Removing an Auto Attendant

To remove an Auto Attendant:

1. Click *NBX Messaging* > *Auto Attendant.*
2. Select the extension, or extensions, that you want to remove and click *Remove Selected*. To select all extensions, enable the *Select* check box.
3. Click *OK*.

You cannot remove the Default Menu Auto Attendant or the Voice Mail Auto Attendant.

Restoring Auto Attendant Greetings

You can restore the greetings to their default values:

- *aamenu.wav* and *aamenu2.wav* prompts
- System-wide Morning, Afternoon and Evening greetings

This feature restores *all* of these prompts and greetings at the same time.

No other user-defined prompt is affected.

To restore greetings, select *NBX Messaging* > *Auto Attendant* and then click *Restore-AA-Greetings*.

Voice Application Setup Utility

The Auto Attendant Voice Application Setup utility provides a series of voice prompts to guide you in configuring your Auto Attendant. You can access the setup utility through any 3Com Business Telephone.

The Voice Application Setup utility is useful for making short-term changes to your Auto Attendant. For example, if you must close your office because of bad weather, you can edit the main menu and direct callers to a message telling them that your office is closed. However, you cannot use the Voice Application Setup to configure submenus. That must be done using the NBX NetSet utility. See "Submenus" on page 212.

Although the setup utility lets you perform tasks in any sequence, 3Com recommends this sequence when setting up the system for first time:

1. Plan the system.
2. Create profiles (phantom mailboxes and destination extensions).
3. Start the Auto Attendant Setup utility.
4. Change the Auto Attendant Setup utility password.
5. Assign actions to key pad buttons.
6. Record greetings and main menu prompts.
7. Set the greeting schedule.
8. Review and test the system.

Using the Voice Application Setup Utility

From a 3Com telephone, you can use the Auto Attendant Setup Utility. Follow these steps:

1. Lift the telephone handset, and then press the *MSG* button to access the Voice Mail system.
2. At the voice mail password prompt, press **`*`**.
3. At the voice mail extension prompt, dial **`999`** if you are using a 3-digit dial plan or **`9999`** if you are using a 4-digit dial plan.
4. Enter the Auto Attendant password. The default password is 0000. 3Com recommends that you change this password.

   `0000 press 1 to assign actions to dial pad key, 9 to record greetings, schedules, change password`

5. Follow prompts to assign key pad button actions, record and play back greetings, change the schedule (morning, afternoon, and evening) and change the Auto Attendant password.

Testing the Auto Attendant

Before using your system, 3Com strongly recommends that you review and test it to verify that all features work as you intend. Use this checklist to verify that your system is ready:

- Do your recorded prompts match your key pad button actions?

  You can define key pad button actions through the NBX NetSet utility (see "Auto Attendant Buttons" on page 215) or through the Voice Application Setup utility.

- Do your time-dependent greetings become active at the times you want?

  If not, you can use the NBX NetSet utility (see "Time-dependent Greetings" on page 210) or the Voice Application Setup utility to change the start times of your morning, afternoon, and evening greetings.

- Do your single-digit transfers and transfer to the general mailbox take a caller to a valid destination?
- When callers reach a mailbox of a single-digit transfer and transfer to the general mailbox, do they hear an appropriate greeting?
- Is someone responsible for checking messages sent to single-digit transfers and transfer to the general mailbox?

- Do you get an "invalid key" message when you press a button that does not have an action assigned?
- Does the Auto Attendant time-out action perform the correct action? Always have a time-out action for a top-level Auto Attendant menu tree. Leaving the time-out action set to *Disabled*, the default, can result in calls being disconnected.
- Do all of your submenu prompts match the submenu key pad button actions?

Voice Profile for Internet Mail

Voice Profile for Internet Mail (VPIM) is an optional feature. Telephone users can use VPIM to send voice mail to a user on any voice mail system that is VPIM-compliant.

The system transmits VPIM voice mail messages by attaching them to e-mail messages. The system then uses SMTP (Simple Mail Transfer Protocol) or ESMTP (Extended Simple Mail Transfer Protocol) to send the e-mail message and its VPIM attachment.

VPIM uses an SMTP server that is embedded in the operating system. To avoid abuse by spammers, always protect an SMTP server with a firewall. Configure the firewall to allow access to UDP port 25 on the system only from valid VPIM systems that need to deliver VPIM messages to the telephone system. The NBX SMTP server is started only when the system has a valid license for VPIM.

VPIM is an optional component that requires a license, which appears in the NBX NetSet Licenses window as *Internet Voice Messaging License*. You must enter a license key through the NBX NetSet utility before you can configure and use VPIM.

Use the NBX NetSet utility to configure VPIM settings, check the status of VPIM queues, and obtain statistics of recent VPIM activity. See these sections for more information:

- Control Parameters
- Operations Management
- Statistics
- Advanced Settings

For information about how to configure the dial plan to use VPIM, see "Dial Plan Configurations and VPIM" on page 302.

Control Parameters

To configure VPIM control parameters, click *NBX Messaging* > *VPIM*.

Table 45 explains the VPIM control parameter fields and their purpose.

Table 45 VPIM Tab Fields

Field	Purpose
Maximum message size (Kbs)	Controls the size of incoming messages from other sites. If a message is larger than the specified value, the system rejects it. The default value represents a voice mail message approximately 4 to 5 minutes in length. **Default:** 3000 KB **Minimum:** 500 KB **Maximum:** 5000 KB
Time between send attempts (Minutes)	For outgoing messages, the system might not be able to contact the target system on the first attempt. If so, the system attempts to contact the target system later. To change the time between attempts to send a voice mail message, change this number. **Default:** 15 minutes **Minimum:** 1 minute **Maximum:** 60 minutes
Maximum number of send attempts	Specifies the number of times the system attempts to connect to the target system. After the specified number of send attempts, the system returns the voice mail message to the sender's voice mail box with an indication that the message could not be sent. **Default:** 4 attempts **Minimum:** 1 attempt **Maximum:** 10 attempts
Maximum time before message expires (Minutes)	**Default:** 60 minutes

Operations Management

To manage the queue of outgoing voice mail messages, click *NBX Messaging* > *VPIM* and then click the Operations Management tab. Table 46 describes the fields in this window.

Some commands require that you start or stop operations. For example, to remove a message from the queue, first stop operations. Similarly,

unless you start operations or they are currently running, you cannot use the "Send all messages now" command.

Table 46 Operations Management Dialog Box Fields

Field	Purpose
Operations status	The status of the queue of outgoing voice mail messages. **Possible values:** Ready, Starting, Processing, Stopped
Number of outgoing messages	The number of messages in the outgoing queue when this dialog box was last accessed or refreshed.
Outgoing Messages	
Remove Selected	Select the voice mail message, or messages, that you want to delete and click *Remove Selected*. To select all voice mail messages, enable the *Select* check box.
Time Waiting	The time that the voice mail message has been waiting in the queue.
# Attempts	The remaining number of attempts to send the message.
Sender	The IP address and extension of the telephone user who sent the voice mail message.
Destination	The IP address and extension to which the voice mail message is to be sent. If a message has multiple destinations, the system lists the first destination followed by three dots. **Example:** 1057@192.168.15.135...
Send all messages now	The system attempts to send all messages immediately, and changes the status of each successfully sent message to *Sent*.
Send all messages now and then delete them	The system attempts to send all messages in the queue and deletes each message that is sent successfully. If a message cannot be sent, it is also deleted.
Delete all messages now	The system empties the queue of all messages
Stop operations	Stops the queue if it is currently active.
Start operations	Starts the queue if it is stopped.

Statistics

The *Statistics* window allows you to view the most recent statistics for voice mail messages.

To view statistics, select *NBX Messaging* > *VPIM* and click the Statistics tab.

Table 47 lists the fields and explains their purpose.

Table 47 Statistics Window Fields

Field	Purpose
Incoming Messages	
Total messages received by system	The number of messages received by this system from voice mailboxes on other systems
Total messages delivered to user mailboxes	The number of voice mail messages delivered to user voice mailboxes on this system. If this number is smaller than the total number of messages received, some messages have not yet been delivered.
Outgoing Messages	
Total messages submitted for external delivery	The number of messages submitted by telephone users of this system for delivery to voice mailboxes on other systems
Total messages delivered to external recipients	The number of messages for which a confirmation of delivery has been received.
Total messages returned to sender on failed delivery	The number of messages that have been returned because they could not be delivered.
Failed Outgoing Messages	The number of messages that never left the queue either because every attempt to deliver them failed and the retry limit was reached, or because the type of failure caused the retry limit to be ignored (example: a non-existent address would be tried only once). If a message had multiple destinations, the first destination is listed, and three dots are displayed immediately after the extension number. **Example:** 1057@192.168.15.135...
Date/Time	The date and time that the message was originally submitted for delivery
# Attempts	The number of attempts that the system has made to send each message
Sender	The person on the local system who created and sent the voice mail message
Destination	The defined target for the voice mail message
Reason	The reason for the most recent failure to deliver the message
Reset and Reboot Times	

Table 47 Statistics Window Fields (continued)

Field	Purpose
Last reset command	The date and time of the last reset command. Sets all VPIM statistics to 0 (zero) and deletes all messages from the Failed Outgoing Messages queue. If this field's date and time are more recent than *Last system reboot*, then the system began to collect the currently displayed statistics at this date and time.
Last system reboot	The date and time of the most recent reboot of the system. A system reboot resets all VPIM statistics to 0 (zero). If this field's date and time are more recent than *Last reset command*, then the system began to collect the currently displayed statistics at this date and time.

Advanced Settings

The system transmits VPIM voice mail messages by attaching them to e-mail messages that are sent using SMTP (Simple Mail Transfer Protocol). You can control the behavior of SMTP and how it sends e-mail messages with VPIM attachments.

To configure SMTP settings, click *NBX Messaging* > *VPIM* and then click the Advanced Settings tab.

Table 48 lists the fields and describes their purpose.

Table 48 VPIM Advanced Settings Dialog Box

Field	Purpose
SMTP OK response	The amount of time that the local system waits for an acknowledgement of a *From* message. After the local system sends a *MAIL* command specifying the sender of the message, it waits for acknowledgement from the other site. The acknowledgement is an *OK* message. **Minimum:** 5 minutes **Default:** 5 minutes

Table 48 VPIM Advanced Settings Dialog Box (continued)

Field	Purpose
SMTP HELO response	The amount of time that the local system waits for an acknowledgement of a HELO message. After the greeting, the local system sends either a HELO (or EHLO to get ESMTP) message to identify itself. The other site then responds with an acknowledgement of that message. **Minimum:** None defined. **Default:** 5 minutes
SMTP EHLO response	The amount of time that the local system waits for an acknowledgement of a EHLO message. After the greeting, the local system sends either a HELO (or EHLO to get ESMTP) message to identify itself. The other site then responds with an acknowledgement of that message. **Minimum:** 0 minutes **Default:** 5 minutes
SMTP MAIL response	The amount of time that the local system waits for an acknowledgement of a MAIL command. After the local system sends out a MAIL command along with the From information, it waits for a response from the other site to indicate that the MAIL command was received. **Minimum:** 5 minutes **Default:** 5 minutes
SMTP RCPT response	The time that the local system waits for an acknowledgement of a RCPT command. When the local system receives and SMTP or ESMTP message, it returns a RCPT command to the sending system for each recipient listed in the *To:* field. **Minimum:** 5 minutes **Default:** 5 minutes

Table 48 VPIM Advanced Settings Dialog Box (continued)

Field	Purpose
SMTP DATA response	The time that the local system waits for an acknowledgement of a DATA command. After the local system has specified all of the recipient information, it sends a DATA command to indicate that it is ready to send the mail message itself. It then waits for the other site to acknowledge the DATA command. **Minimum:** 2 minutes **Default:** 2 minutes
SMTP DATA END response	The time that the local system waits, after sending the entire message, for an acknowledgement from the other site that the message was received. After the local system sends the entire message, it sends a single dot (ascii code 056) to the other site. It then waits for an acknowledgement from the other site that the dot has been received. **Minimum:** 10 minutes **Default:** 10 minutes
SMTP RSET response	The time that the local system waits for an acknowledgement of a RSET command. Maintaining a cached connection between the local system and any other site requires additional system resources compared to a non-cached connection. If connection caching is enabled, the local system waits for the defined time-out period and if no message is received, it sends a RSET command to the other site. **Minimum:** None defined. **Default:** 10 minutes
SMTP QUIT response	The time that the local system waits for an acknowledgement of the QUIT command. When the local system transmits a message and wants to break the connection, it sends a QUIT command. It then waits for the other site to acknowledge the QUIT command. When the acknowledgement arrives, or when the time-out value is reached, whichever comes first, the local system breaks the connection. **Minimum:** None defined. **Default:** 5 minutes

Configuring Domain Name Server Information

When the SMTP utility attempts to send e-mail, it must be able to resolve a host name within an e-mail address and determine the proper IP address from that name. Domain Name Servers on the Internet perform this function. You can configure up to three DNS entries with the NBX NetSet utility. The system uses the second and third entries if the first or second cannot be reached. To configure DNS information in the NBX NetSet utility:

1. Click *System-Wide Settings* > *IP Settings*.
2. In the *Primary DNS*, *Secondary DNS*, and T*ertiary DNS* fields, type the IP addresses of three Domain Name Servers. If you have the IP address of only one server, type it in the *Primary DNS* field. If you have the IP address of only two servers, type them in the *Primary and Secondary DNS* fields. Click *OK*.

10 SIP-MODE OPERATIONS

NBX systems that use Session Initiation Protocol (SIP) are described in these topics:

- Overview of SIP Mode on the NBX Platform
- Other Applications Support
- Enabling and Configuring SIP Mode
- Adding Telephone Users and Devices

For more information about these topics and configuration procedures, see the online Help.

Overview of SIP Mode on the NBX Platform

A system running release R6.0 or higher can operate using two forms of Call Control /Setup.

- **3Com call control mode** — The traditional call control employed by all previous releases of the system software.
- **SIP mode** — 3Com telephones and line cards communicate with the system using 3Com call control mode. SIP devices, such as the 3Com 3108 Wireless Telephone, generic SIP phones, and SIP gateways and servers, use IETF RFC 3261 (SIP: Session Initiation Protocol) to communicate with the system.

When you configure a system to run in SIP mode, all audio is carried using RFC 1889 (RTP: A Transport Protocol for Real-Time Applications) as the underlying communications infrastructure. Some older devices do not support RTP and are disabled when you enable SIP mode operations. For more information about supported devices in SIP mode, see "Device Support Details" on page 234.

SIP Mode Operations

A SIP mode system has these operating characteristics, limitations, and features that differ from a 3Com call control mode system:

- SIP mode is not supported on the NBX 100. See Table 50 on page 236 for detailed system platform support information.
- SIP mode on an NBX system means standard SIP support (RFC 3261) with no proprietary extensions to SIP. Third-party telephone features that are dependent on non-standard SIP will not work. A SIP mode system does not support secure SIP signaling or secure RTP. It does not support NAT, firewalls, or RTP relay. Communication is over UDP only.
- A SIP mode system uses Standard IP as the network protocol. If you enable SIP on a system that uses Ethernet mode or IP on the Fly, the system automatically switches to Standard IP. You typically configure a DHCP server to provide IP information to devices and configure Option 184 on the DHCP server to provide the Call Processor IP address.
- A SIP mode system can interoperate with any other SIP endpoint, including gateways, devices, and SIP-enabled applications. For example, a SIP mode system is able to interoperate with the 3Com VCX Telephony System, a SIP-based system designed to support large distributed enterprises.
- 3Com Telephones connected to a SIP mode system behave the same as they do when running under 3Com call control mode except for these differences:
  - Conferences can include up to three parties, the conference originator, and two other conference parties, either internal or external. The limit is four parties on a system that is not running in SIP mode. However, the number of simultaneous conference sessions supported in SIP mode increases beyond the current limit of 12. For support for conferences that require more than 3 parties, you can configure the optional 3Com IP Conferencing Module.
  - In SIP mode, the conference originator cannot forward, transfer, camp on, or park a conference call.
  - The WhisperPage feature is not available on a system running in SIP mode.
  - An external messaging application, typically the 3Com IP Messaging Module, provides Voice mail and Auto Attendant menus and prompts, and Music-on-Hold. NBX Messaging is disabled when you enable SIP.
- If you do not use an external conference server, these devices can participate in a conference call:
  - 3Com 3108 Wireless Telephone

  - Generic SIP telephones
  - 3Com pcXset Soft Telephone Client
  - Analog telephones

  However, you cannot use these devices to add extensions to a conference.

- ATA devices and the 3Com pcXset Soft Telephone Client cannot initiate a conference on a SIP mode system.
- The Auto Discovery feature works for 3Com phones (except the 3108 Wireless Telephone), and cards and devices. You must configure SIP devices and gateways, and the 3Com 3108 Wireless Telephone manually. Typically, you use NetSet utility to add the telephone user and user extension to the system database. You specify the extension and the IP, and authentication parameters that the SIP device uses to communicate with the Call Processor on the SIP device itself.
- NBX Messaging does not work on a system running in SIP mode. A SIP mode system must have an external messaging system to provide voice mail and Auto Attendant services. 3Com recommends the 3Com IP Messaging Module. On a system running 3Com call control mode, you need an optional license to run an external messaging system. If you enable SIP mode on a system, no external messaging license is required.
- A telephone user can login at different phones (Hot Desking), but only one login at a time is allowed. If a telephone user is on a call, and then logs into another phone, the system disconnects the first call. This feature works only on generic SIP telephones and the 3Com 3108 Wireless Telephone. This feature is not available on a system that is running 3Com call control mode.
- For Emergency 911 calls, you can configure a 3Com telephone to use an alternate SIP gateway if one is available to connect calls if the system is down. 3Com telephones do not support the DHCP option for providing an alternate SIP gateway address, so this feature requires manual configuration on the telephone.
- Button mapping is not supported for the 3Com 3108 Wireless Telephone or generic SIP telephones. You cannot map a CO Line to a generic SIP telephone or a 3108 Wireless Telephone.
- The 3Com 3108 Wireless Telephone or generic SIP telephones cannot be bridged extensions.

- Virtual Tie Lines are not available on a system running in SIP mode. However, you can achieve the same result, connecting different systems, by configuring each system that is running SIP mode as a trusted SIP interface. A trusted SIP interface can include SIP proxies, SIP applications, SIP gateways, and any other third-party SIP device, including 3Com VCX IP Telephony systems. Telephone communication between the NBX and VCX systems supports Make Call, Receive Call, and Call Hold. Each NBX system can use the same IP Messaging Module.
- A Trusted SIP Interface connection between an NBX system and a 3Com VCX telephone system can share the same IP Messaging Module. However, the automatic mailbox creation process can work for only one type of system. Typically, you use automatic mailbox creation for the enterprise-class VCX system and manual mailbox creation for the NBX system or systems.
- Paging is supported on 3Com phones (except the 3Com 3108 Wireless Telephone) with SIP enabled. Generic SIP phones and the 3108 Wireless Telephone can neither initiate nor receive pages.
- There are restrictions on the Automatic Call Distribution (ACD) feature on a SIP mode system. See "SIP Mode and ACD" on page 239.
- Directory services are not supported on generic SIP phones and 3Com 3108 Wireless Telephones.
- SIP mode systems support Attendant Console operations. However, only call status, not line status, of SIP endpoints is available for SIP telephones.
- A TAPI application is only able to *monitor* generic SIP phones and the 3Com 3108 Wireless telephone.

A SIP mode system supports E-911 functionality. However, for 911 calls, you must manually configure generic SIP telephones and the 3Com 3108 Wireless Telephone to use the alternate SIP gateway address if the Call Processor is not available. For generic SIP telephones, this behavior is specific to the telephone, and it is the responsibility of telephone to provide this functionality.

Device Support Details

There are important distinctions to keep in mind when you consider how devices connected to a SIP mode system behave:

- SIP-only telephones such the 3Com 3108 Wireless Telephone and generic, third-party SIP telephones can use many of the standard telephony features through feature codes.

- Legacy devices that do *not* support RTP become disabled if they are connected to a system that is running in SIP mode. When you enable SIP mode, the system displays a report that lists any device that will be disabled. Table 49 shows the devices that can support the full feature code set:

Table 49 Devices Supported in SIP Mode Operation

Device	Part Number
2102B/PE Business Phone	3C10226B/PE or 3C10228IRB/PE
1102B/PE Business Phone	3C10281B/PE
2101B/PE Basic Phone	3C10248B/PE
3100 Entry Phone	3C10399A and 3C10399B
3101 and 3101SP Basic Phone	3C10401A and 3C10401SPKRA 3C10401B and 3C10401SPKRB
3102 and 3102B Business Phone	3C10402A and 3C10402B
3103 Manager's Phone	3C10403A and 3C10403B
3106C and 3107C Cordless Phones	3C10406A and 3C10407A
pcXset Soft Telephone Client	3C10316 and 3C10154
1-port Analog Terminal Adapter	3C10400A and 3C10400B
V3000 Analog ports	3C10600A and 3C10600B
V3000 BRI-ST ports	3C10601A
V3001R System ports	3C10602A
4-port Analog Terminal Card	3C10117C
Analog Line Card	3C10114C
T1 Digital Line Card	3C10116D
E1 Digital Line Card	3C10165D
External Paging Device	N / A
NBX Media Driver	3C10319
Polycom Soundstation IP 4000	2200-06632-001

Feature Support

The 3Com devices listed in Table 49 can take advantage of the full feature set that the system offers. Generic SIP telephones and the 3Com 3108 Wireless Telephone support some features through feature codes. However, any feature code that must be activated while a call is in progress is *not* supported.

See the *NBX Feature Codes Guide for SIP Telephones* for complete information about how generic SIP telephones and the 3Com 3108

Wireless Telephone interact with the standard features. The guide is available to end users and the system administrator through the NBX NetSet utility.

Hot Desking

Hot desking refers to the ability of a SIP telephone user to enter the username and password on a different telephone, and have that telephone come up as his or her own. This is one advantage of using a SIP telephone.

However, there are several things to remember in a hot-desking scenario:

- To support hot desking, the system de-registers the telephone user from the previous telephone, but the previous telephone must not be in use in order for the de-registration to take place.
- The behavior of the system services might be different for the telephone user if the new telephone is a different type.
- The telephone user can use the NBX NetSet interface to change the extension of the new telephone, but it is the responsibility of the telephone user to change the extension on the telephone itself to effect synchronization. Otherwise, the system cannot authenticate the telephone and it is inoperative.

Platforms Supported

Because SIP mode operation increases memory demands on the system, V3000 and V5000 systems support SIP mode operations only if they have the optional memory upgrade installed. Table 50 lists the system platforms, and their memory configurations, that are capable of operating in SIP mode:

Table 50 System Platforms Supporting SIP Mode

Call Processor Model	SIP Capable?
NBX 100	No
V5000 - 128MB	No
V5000 - 640 MB)	Yes
V3000 Analog or BRI-ST - 128MB	No
V3000 Analog or BRI-ST - 640MB	Yes
V3001R	Yes

To determine if your V3000 or V5000 system has the memory upgrade installed:

1. Log in to the NBX NetSet utility using the administrator login ID and password.
2. Click *System-Wide Settings* > *System Identity.*
3. Verify that **Memory Upgrade Installed** is set to `YES`.

Licensing and Resource Limits

This section describes the system resource limits on a SIP mode system.

Sessions

A SIP *session* is an end-to-end communications path between two endpoints. A session includes a voice mail transaction, a public or restricted conference, or a gateway path. There is a maximum limit of 300 concurrent sessions on a SIP mode system.

When you configure a SIP mode system, be careful about how many simultaneous sessions you allow for each feature for which you can configure sessions. For some NetSet SIP-related functions, such as messaging and conference configuration, you must estimate the number of s*imultaneous sessions* that the feature is likely to manage. For example, if you estimate that the system is likely to manage up to 30 simultaneous voice mail messages, the system blocks the thirty-first message.

The number of simultaneous sessions that you specify for a feature counts against the total device limit for the system. You can determine the number of devices used against the total number in the Usage Report (click *Licenses and Upgrades* > *Licenses)*. V3000 and V5000 systems with expanded memory and V3001R systems can be licensed to manage up to 1500 devices.

Devices

Devices count against the number of licenses allowed in a group (Group 0 – 4). Each telephone consumes one license from the appropriate group's limit.

Gateways

Gateways do not count against the device limit itself. Instead, the number of sessions on the gateway is counted. For example, if you create a

gateway with three sessions, those three sessions immediately count against the device limit. You add gateways as Trusted SIP Interfaces.

SIP Mode License Requirements

This section details the licensing requirements for a system running in SIP mode. You do not need a license to enable SIP mode operation or for external messaging or conferencing applications.

- A 3Com 3108 Wireless Telephone uses a Group 1 license and counts as one system device.
- Each third-party SIP phone uses one Group 1 license and counts as one system device.
- Each 3Com telephone uses a Group 1 license and counts as one system device.
- A third-party PSTN gateway requires one system device license for each audio path trusted interface.

  SIP gateways, SIP proxies, and third-party SIP applications can be assigned as trusted interfaces.

  At initial configuration, each trusted interface must assign the maximum number of audio paths that it can have open concurrently. Each audio path is tracked against the licensed system capacity device limit of up to 1500 devices. For example, if the trusted interface is configured for thirty audio paths, the thirty-first request receives a busy tone or is redirected to another Dial Plan route, if one is configured and available.
- Multi-vendor SIP soft trunks (such as Cisco VIC Cards, VCX-to-NBX-to-VCX dial plans, and MCI SIP trunks) require one system device license for each audio path trusted end point.

Dial Plan Considerations

The Dial Plan consists of the rules that govern calling behaviors. the NBX NetSet utility automatically updates your dial plan for most SIP related changes. However, you must manually update the dial plan if you add a 3Com IP Conferencing Module to the system.

The default dial plan includes an additional default entry, SIP Connection Ports, in the routing table. A SIP Connection Port identifies the route for a call going to a SIP gateway or to another trusted device.

SIP Mode and ACD

Generic SIP telephones and the 3Com 3108 Wireless Telephone do not fully support the ACD feature. The following applies to SIP-only devices and their interaction with ACD:

- A generic SIP phone and the 3108 Wireless Telephone cannot call into or be a member of an ACD group.
- A generic SIP phone and the 3108 Wireless Telephone cannot call into or be a member of a Hunt group or a Calling group.

ACD Features Not Available on SIP Mode Systems

These ACD features are not available on a SIP mode system:

- In Queue Digit processing
- Queue Exit announcement
- Estimated Wait time Announcement
- Business and custom hours
- Shifts
- Wrap-Up Time
- Closed announcement

Other Applications Support

This section lists how SIP-mode supports other applications on the system.

Call Log Support

SIP telephones themselves provide call log information. That is, the system does not communicate information related to call logs to SIP endpoints.

SNMP Support

The system stores information about SIP telephones, which is delivered to the SNMP manager by means of proxy information managed by the system.

SysLog Support

A SIP mode system supports Syslog functionality.

CDR Support

For SIP devices, call data records might display `Not reachable` as the release cause if the device is offline. CDR provides the complete URL rather than extensions only for SIP telephones.

Enabling and Configuring SIP Mode

To enable a system to run in SIP mode is a one-step process that has extensive affects on the system. There is a significant impact on existing telephone users if you convert an existing operating NBX system to SIP mode, particularly on Auto Attendants and voice mail. Because NBX Messaging is not available on an NBX system operating in SIP mode, you must reconfigure those services. All existing voice mail configuration and messages are lost. In addition, many older 3Com telephones and devices cannot support SIP and will be disabled on a SIP mode system.

The following topics describe how to enable and configure SIP and add devices:

- Install and Configure the System for SIP Mode
- Enable SIP Mode
- Add Messaging
- Configure Music on Hold
- Configure Auto Attendants
- Configure ACD Delayed Announcements
- Add Trusted SIP Interfaces
- Add an Optional IP Conferencing Module

Install and Configure the System for SIP Mode

To install and configure the system for SIP mode:

- Follow the procedures in the *NBX Installation Guide* to power up the system and configure network connectivity.
- Configure the system-wide settings, such as the system date and time, business identity settings, and so forth.
- Install the 3Com IP Messaging Module, which is described in the *IP Messaging Installation Guide* (click *Downloads* > *Documentation*).

Enable SIP Mode

To enable SIP mode on your system:

1. Log in to the NBX NetSet utility using the administrator login ID and password.
2. Click *System-Wide Settings* > *Enable Features System-Wide*.
3. Enable the *Enable SIP* check box, and then click *Apply*.
4. Click *OK*.

At this point the system performs these steps:

- Backs up the database.
- Reboots automatically after the backup is complete.
- Enables Standard IP.

  The system running in SIP mode must use Standard IP as its network protocol. The system disables IP On-The-Fly and Ethernet and makes them unavailable. All telephones operate at Layer 3.
- Enables the Third-Party Messaging option in *System-Wide Settings* as part of the reboot process.

  The Third Party Messaging option does not require a license in SIP mode. The NBX Messaging option is disabled and unavailable in SIP mode.

Disabling SIP Mode

To convert a SIP mode system to a 3Com call control mode system:

1. Log in to the NBX NetSet utility using the administrator login ID and password.
2. Click *System-Wide Settings* > *Enable Features System-Wide.*
3. Clear the *Enable SIP* check box, and then click *Apply.*

   The system queries if you want to restore the database from a previously-stored backup. If you do not select a previously-stored backup, the system uses the default backup database when it reboots.

Caution: *When you enabled SIP mode, the system created a backup database for you. If you disable SIP mode, you can use that same backup database to restore the system to its pre-SIP mode state. However, if you use the default backup database, the system will not be restored to the state it was in before you converted the system to SIP mode because non-RTP device data cannot be restored by default.*

4. Click *OK*.

   You have chosen to run in 3Com call control mode. At this point, the system:

   - Backs up the database.
   - Reboots automatically after the backup is complete.
   - Enables Ethernet as a part of the reboot process. (You can change this setting if you wish.)

- Enables NBX Messaging.

The system now reverts to 3Com Call Control mode. SIP-only devices no longer function, and the database has changed.

Add Messaging

A system running in SIP mode must have an external messaging system. 3Com recommends that you use the 3Com IP Messaging Module, which has been enhanced to support system operations.

After you configure IP Messaging on the system, you must configure the services — Auto Attendants, Music on Hold, and ACD announcements.

For information about how to install and configure services on the 3Com IP Messaging Module, see the IP Messaging Module Installation Guide*, which is available through the NBX NetSet utility (click* Downloads > Documentation*). Other IP Messaging documentation for administrators and end users is available on the NBX Resource Pack.*

To add IP Messaging to a system:

1. Log in to the NBX NetSet utility using the administrator login ID and password.
2. Click *SIP Applications* > *IP Messaging*.
3. Type the extension used by the system for IP Messaging. This extension must be an unused extension on the system in the range of external extensions, 6000-7999 in a 4-digit dial plan. The system adds the extension to the *0003 extension list in the dial plan.

   Every physical and virtual device on a system must have an extension. The IP Messaging extension identifies the IP Messaging Module, a trusted SIP interface. To verify the dial plan change, click *Dial Plan* > *Extension List,* and then click extension list *0003.
4. Type a description for the IP Messaging Module.
5. Type the eth0 IP address for the IP Messaging Module. NBX configurations do not use the eth1 interface.
6. Type a port number for IP Messaging. A SIP endpoint is identified by the IP and port combination.

   The default port, 5060, is listed in the Internet Assigned Number Authority port list as a Registered Port for SIP.
7. Type the maximum number of simultaneous sessions. This value is less than or equal to the number of available IPM licenses. Each session

requires one system device license. See "Licensing and Resource Limits" on page 237 for more information.

8 Type the voice mail extension that end users can dial to access the Auto Attendant.

9 Type the interval for subscriber data updates to the IP Messaging Module.

Subscriber data uploads only if extension numbers are unique. System subscriber data is written to an XML file at the specified interval. See the next topic, "Mailbox Creation Details" for further details.

10 Type the password (the default password is *nice*), that is used to access the IP Messaging Module.

11 Click *Send Update Now* for an immediate upload of subscriber data to the IP Messaging Module.

12 Click *OK* or *Apply* to save your changes.

When you click *Apply*, the system adds the IP Messaging Module as a trusted endpoint. Click *SIP Applications* > *Trusted SIP Interfaces* to verify.

Mailbox Creation Details

When you use the NBX NetSet utility to create a new telephone user, the system communicates with the IP Messaging Module, which then creates a new mailbox. This communication method from the system to the IP Messaging Module is not in real time. The system creates an XML file that includes the new user information and sends it to the IP Messaging Module at defined intervals. You can also manually execute an immediate file transfer. At defined intervals (the default is every six hours), the IP Messaging server collects the XML files from one or more systems, combines the information into one update file, and then creates the new mailboxes. The process incudes these steps:

- When you create a new telephone user or a new trusted interface on the system, the system creates an XML file that includes all the information that the IP Messaging Module requires to create a corresponding mailbox. The file is named `<NBXSYSID>_nbxuserpwd.xml`.
- If a new file has been created, that is, if the system needs to create new mailboxes on the IP Messaging Module, the system transfers the file to the IP Messaging Module at defined intervals. The interval is set in the NBX NetSet utility (click *SIP Applications* > *IP Messaging)*. You can also force an immediate update from this window.

- The system uploads the XML file to the IP Messaging Module through a secure FTP connection, which is stored in the **/usr/app/import** directory.
- At a defined interval (the default is every 6 hours) the IP Messaging Module combines all the XML files it has received and creates or updates mailboxes on the IP Messaging Module. These files can be multiple files from a single system or files from more than one system.
- A copy of the combined XML file (`nbx-user-combined.xml`) is stored on the IP Messaging server in the **/usr/app/export** directory.

Telephone users can use the 3Com IP Messaging Module to change their voice mail password. This results in different passwords for logging into the NBX NetSet utility and the IP Messaging voice mail system. Telephone uses are responsible for changing their NetSet login password to synchronize with their voice mail password.

Configure Auto Attendants

You must configure the system to use the Auto Attendant services of the IP Messaging Module. This section describes how to configure IP Messaging on the system. For instructions about how to configure the IP Messaging server to operate with the system, see the *IP Messaging Module Installation Guide*, which is available through the NBX NetSet utility (click *Downloads* > *Documentation*).

The IP Messaging Module includes a default Auto Attendant and you can create your own customized Auto Attendants. You must configure the Auto Attendant settings on the IP Messaging Module before those services are available to the system. For information about how to creating Auto Attendants, see the *IP Messaging Operations and System Administration Guide.*

To specify an IP Messaging Auto Attendant on the system:

1. Log in to the NBX NetSet utility using the administrator login ID and password.
2. Click *SIP Applications* > *IP Messaging*, and then click the Auto Attendant tab.
3. To add a new Auto Attendant, click *Add*. To modify an existing Auto Attendant, click the Auto Attendant's mailbox number (or port number).
4. Specify an Auto Attendant Mailbox and a description of that mailbox.

Before this Auto Attendant can be operational, you must use the appmon configuration program to configure the Auto Attendant on the IP Messaging Module. When you assign a mailbox to the Auto Attendant, you must specify the same mailbox number you entered in the NBX NetSet utility.

5 Click *OK* or *Apply* to save your changes.

Configure Music on Hold

The external IP Messaging Module provides Music on Hold (MOH) and Music on Transfer (MOT) services for a SIP mode system. However, there is a practical limit in enabling these features because the IP Messaging application has a limit of 300 ports for sessions at any one time.

You must configure the MOH/MOT settings on the IP Messaging Module before those services are available to the system. For information about how to create MOH/MOT service on the IP Messaging Module, see the *IP Messaging Operations and System Administration Guide*.

To configure mailbox information for the Music on Hold (MOH) and Music on Transfer (MOT) services on the system:

1 Log in to the NBX NetSet utility using the administrator login ID and password.

2 Click *SIP Applications* > *IP Messaging,* and then click the Music On Hold tab.

3 Select the MOH and MOT options and provide the mailbox number that the IP Messaging Module uses to provide music service. You must provide a mailbox number if either the Music on Hold or Music on Transfer check boxes are enabled.

4 Click *OK* or *Apply* to save your changes.

Before the services can be operational, you must use the appmon configuration program to configure the services on the IP Messaging Module. When you assign a mailbox to the services, you must specify the same mailbox number you entered in the NBX NetSet utility.

Configure ACD Delayed Announcements

If your system is operating in SIP mode, you must use an external messaging application to provide Automatic Call Distribution (ACD) announcements. A system running in SIP mode supports ACD Open/Closed announcements. It does not support estimated wait-time announcements or In-Queue Digit Processing. For more information, see Chapter 7, "Call Distribution Groups" on page 135.

SIP Telephone Restrictions and ACD

These restrictions apply to SIP-only devices and their interaction with ACD:

- A SIP-only phone cannot call an ACD group.
- A SIP-only phone cannot be a member of an ACD group.
- A SIP-only phone cannot call a Hunt group or a Calling group.
- A SIP-only phone cannot be a member of a Hunt group or a Calling group.

ACD Features Not Available in SIP

These ACD features are not available on a SIP mode system:

- In Queue Digit processing
- Queue Exit announcement
- Estimated Wait time Announcement
- Business and custom hours
- Shifts
- Closed announcement

Incoming ACD Calls From a SIP Gateway

Calls coming in to an ACD group from a SIP gateway exhibit the same behavior as incoming calls from any other source. However, do not set the call coverage for that ACD to a 3Com phone. An ACD group's call coverage can be:

- Another ACD group
- Hunt group
- Sip phone

ACD Announcement on a SIP-Mode System

You must configure ACD Announcements on a SIP-mode system on the IP Messaging Module. The following is a brief explanation of the Delayed Announcement functionality with 3Com IP Messaging Module:

1 Configure the 3Com IP Messaging Module for the various announcements.

Each announcement is assigned to a mailbox on the 3Com IP Messaging Module. This is a read-only mailbox. When the mailbox receives a call, the mailbox plays the announcement assigned to it. Announcements can be imported, or they can be recorded to the 3Com IP Messaging Module.

The telephone user can use the IP Messaging facility to record announcements. The system administrator is responsible for configuring the mailboxes on IP Messaging with appropriate announcements.

For example, assume that IP Messaging is configured as follows:

Table 51 Example ACD Mailboxes

Mailbox Name	File Name
Mailbox1	welcome.wav
Mailbox 2	sales.wav
Mailbox3	support.wav
Mailbox4	ProductInfo.wav
Mailbox5	Phones.wav

2 Set up the Delayed Announcements for the ACD groups.

the NBX NetSet utility lets you map Mailbox numbers (present on IP Messaging) to an Announcement Description (click *SIP Applications* > *Announcements*).

Keeping with this example, assume that you create an ACD Group that plays announcements regarding telephone information. Therefore, ACD is configured to use the announcements on Mailboxes 1, 4, and 5. To accomplish this you must configure the announcements as follows:

Mailbox	Announcement Description
Mailbox1	Welcome to 3Com
Mailbox4	Product Information
Mailbox5	Phones Information

3 Go to the Announcements configuration page for the ACD Group in order to do the announcement assignment.

The interface is similar to the voice mail page except that the *Filename* field is the *Announcement Description* field, and this field provides the list of the configured announcements. Therefore, you simply need to provide the timeout parameters and select the Announcement Description from the drop-down list, as follows:

Announcement Description	Timeout
Welcome to 3COM	45sec
Product Information	50sec
Phones Information	60sec

4 If a caller dials the ACD group extension and is placed in the ACD queue, the system plays the Delayed Announcements as they were configured using the 3Com IP Messaging Module.

For each different Announcement the systems makes a call to the appropriate 3Com IP Messaging Module Mailbox (a URL, such as Mailbox@ipms.com). In the above case, new requests are sent to the IP Messaging Service after each timeout. Therefore, the IP Messaging Service receives 3 requests:

- Mailbox1@ipms.com
- Mailbox4@ipms.com
- Mailbox5@ipms.com

Adding and Modifying Announcement Mailboxes

To add or modify an announcement mailbox on the system:

1 Log in to the NBX NetSet utility using the administrator login ID and password.

2 Click *SIP Applications > IP Messaging,* and then click the Announcements tab.

3 To add a new auto announcement, click *Add*. To modify an existing announcement, click the mailbox number (port number) of the announcement you want to modify.

4 Click *OK* or *Apply* to save your changes.

Before the services can be operational, you must use the appmon configuration program to configure the service on the IP Messaging

Module. When you assign a mailbox to the services, you must specify the same mailbox number you entered in the NBX NetSet utility.

Add Trusted SIP Interfaces

Trusted SIP Interfaces may be SIP gateways, other NBX systems, 3Com VCX telephone systems, Call Processors or other trusted interfaces. Each interface you add and how you configure it affects your device licensing. Each audio path trusted end point requires one system device license. See "Licensing and Resource Limits" on page 237 for more information.

You do not add telephones as trusted interfaces. For information about how to add 3Com telephones and generic SIP telephones to the NBX SIP mode system, see "Adding Telephone Users and Devices" on page 253.

To add or modify a trusted SIP interface:

1. Log in to the NBX NetSet utility using the administrator login ID and password.
2. Click *SIP Applications* > *Trusted SIP Interfaces*.
3. Click *Add* to add a new trusted interface or click an extension from the list to modify that trusted interface.

Add an Optional IP Conferencing Module

SIP mode operations support only 3-party conferences. You can add an external conferencing server, such as the 3Com IP Conferencing Module, to expand your system's conference capabilities. The 3Com IP Conferencing Module supports up to 25 telephones in a conference.

The IP Conferencing Module supports two types of Meet-Me conferences:

- **Public** — Public conferences are dial-in conferences in which a caller can dial a conference extension and connect directly to the conference.
- **Restricted** — Restricted conferences are secure conferences. Callers must authenticate themselves before the system allows them to join a conference. The system connects a caller to the IP Conferencing Module Attendant, which requires the caller to provide a Conference ID and a password.

Use the NBX NetSet utility to configure IP Conference Server and Conference Attendant settings:

- 3Com Conferencing servers use different UDP ports for Restricted and Public conferences. Therefore, you must configure these ports separately in the NBX NetSet utility.
- You must configure a dedicated conference extension to enable callers to connect to the IP Conferencing Module Attendant.
- Each conference you add is a trusted SIP interface, which the system includes in the Trusted SIP Interfaces list.
- You must edit your dial plan to complete the 3Com IP Conferencing Module configuration.

To configure IP Conference Server:

1. Log in to the NBX NetSet utility using the administrator login ID and password.
2. Click *SIP Applications* > *3Com IP Conferencing Module.*
3. Type the extension that the system uses for IP Conferencing. This extension must be an unused extension on the system in the range of external extensions, 6000-7999 in a 4-digit dial plan. You must use a different extension from the one you use to configure the Conference Attendant settings.
4. Type a description for the IP Conferencing Module.
5. Type the IP address for the IP Conferencing Module.
6. Type a port number. A SIP endpoint is identified by the IP and port combination.

   Port 5060 is set as the default during installation and typically does not need to be changed.
7. Type the maximum number of simultaneous sessions. Each session requires one system device license. See "Licensing and Resource Limits" on page 237 for more information.
8. Click *OK* or *Apply* to save your changes.

   When you click *Apply*, the system adds a trusted endpoint. Click *SIP Applications* > *Trusted SIP Interfaces* to verify.
9. Configure the dial plan.

   You must add an extension list to the dial plan to support routing of extensions to the conference server or edit the extension list, if one has

already been created. For more information see "Dial Plan and 3Com IP Conferencing Module Configuration" on page 252.

To configure the settings of the Conference Attendant for restricted conferences:

1. Log in to the NBX NetSet utility using the administrator login ID and password.
2. Click *SIP Applications > 3Com IP Conferencing Module,* and then click the Conference Attendant Settings tab.
3. Type the extension that the system uses for IP Conferencing. This extension must be an unused extension on the system in the range of external extensions, 6000-7999 in a 4-digit dial plan. You must use a different extension from the one you used to configure the IP Conference Server settings.
4. Type a description for the IP Conferencing Module.
5. Type the IP address for the IP Conferencing Module.
6. Type a port number. A SIP endpoint is identified by the IP and port combination.

   Port 5092 is the port number defined in the IP Conferencing server for running the Conference Attendant.
7. Type the maximum number of simultaneous sessions. Each session requires one system device license. See "Licensing and Resource Limits" on page 237 for more information.
8. Click *OK* or *Apply* to save your changes.

   When you click Apply, the system adds a trusted endpoint. Click *SIP Applications > Trusted SIP Interfaces* to verify.
9. Configure the dial plan. You must add an extension list to the dial plan to support routing of extensions to the conference server or edit the extension list if one has already been created. For more information see "Dial Plan and 3Com IP Conferencing Module Configuration" on page 252.

Dial Plan and 3Com IP Conferencing Module Configuration

You must configure the dial plan to complete the 3Com IP Conferencing Module configuration. The following procedure describes the process. For complete dial plan information, see "Dial Plan" on page 257.

1 Add an extension list to the dial plan to support routing of extensions to the 3Com IP Conferencing Module.

For example, you can define the 3Com IP Conferencing Module extension list as follows:

```
/                            Route      Description
/                            -----      -----------
DestinationRoute Create      900        Conference

/                            Route   Entry   DestinationExtension
/                            -----   -----   -------------------
DestinationRouteEntry Create   9     1       *0900

/ Extension List *0900 holds the internal extension of 3Com IP Conferencing Module
```

2 Create a route entry in the dial plan for the dialed-in digits the telephone user of the 3Com IP Conferencing Module enters.

For example, using the extension list created in Step 1, the entry below shows a dial-in that begins with 900.

```
/                   ID   Entry   Digits  Min  Max  Class      Prio    Route
/                   ---  -----   ------  ---  ---  -----      ----    -----
Table Entry Create  1    6       900     3    3    internal   0       900
```

Therefore, if the caller dials 900, the system receives the extension of the 3Com IP Conferencing Module and the port number for the private conference from the dial plan. The system can route the call to the 3Com IP Conferencing Module.

3Com Public IP Conferencing Module Configuration

You must configure the dial plan to complete the 3Com Public IP Conferencing Module configuration. The dial plan uses the private conference dial plan if it is configured; otherwise, you need to configure the dial plan for Public conference.

The only change required is in the dial plan prefix entry table because in a Public conference, you need to define a range of extensions rather than a single extension.

For example, using the above configuration and taking the case that the extensions range from 700-799, the table entry can be as follows:

```
/                    ID   Entry   Digits  Min  Max  Class      Prio    Route
/                    ---  -----   ------  ---  ---  -----      ----    -----
Table Entry Create   1    7       7       3    3    internal   0       900
```

If the caller dials 700, the system receives the extension of 3Com IP Conferencing Module and the port number for the Public conference from the dial plan. The system can route the call to the 3Com IP Conferencing Module.

Adding Telephone Users and Devices

This section explains how to add a generic SIP telephone or a 3Com 3108 Wireless Telephone to a SIP-mode system. For information about how to add other types of 3Com telephones, see "Telephone Configuration" on page 93, which describes how to add devices manually or by using the Auto Discovery feature. The procedures apply to both SIP mode and 3Com call control mode systems. However, because the 3Com 3108 Wireless Telephone is a SIP device, you cannot use Auto Discovery to add it to the system. See "Adding a 3Com 3108 Wireless Telephone" on page 255 for information about how to add a 3108 to a SIP mode system.

Adding a Generic SIP Telephone

To add a generic SIP telephone to the SIP mode system,

- Add a new telephone user and extension to the system and then configure the telephone with that username, the default password (1234) and the extension. If you are not using a DHCP server, you might need to configure IP connection information.
- Configure the SIP telephone with system data, such as the system IP address and UDP port authentication information, and the extension you created in the NBX NetSet utility.

  The SIP telephone has configuration interface that lets you configure it. Most generic SIP telephones include an embedded web server that enables you to connect to the phone directly and configure authentication and feature settings. After you configure the SIP

telephone, it uses the authentication information you provided to register with the system and is a member of the Telephones list (click T*elephone Configuration > Telephones)*.

To add a generic SIP telephone:

1. Log in to the NBX NetSet utility using the administrator login ID and password.
2. Click *User Configuration* > *Users* > *Add*.
3. Specify telephone user information and an unused extension.

   When you click *OK* or *Apply*, the system creates the telephone user with a default password of 1234.
4. Connect the telephone to power and the network. Use the telephone documentation to configure basic network connectivity.

   Typically, your phone gets its address from a DHCP server. You can use the telephone controls to view the phone's IP address. Scroll through the phone's menus until you find a display such as *preferences* or *Network Info*.
5. After you find the telephone's IP address, open a browser and type it into the address line.

   Most, but not all telephones, include an embedded web server for local configuration. Be sure to consult the telephone's documentation if you cannot access the its configuration interface.
6. After you connect to the telephone's configuration interface, find and configure connections settings. For example, on a Sipura telephone, you click the `Admin Login` link, and then click the `Ext.1` tab to access these settings:

Proxy	Specify the IP address of the NBX server. This field might also be known as SIP Proxy.
Display Name	Typically, you specify the extension, although this is not required.
Password	Specify the default password, 1234. The telephone user can by log in to the NBX NetSet utility and use the extension as the username and this password to change the password. Do not use the telephone user interface to change the password because that password change is not passed to the database.
User ID	Specify the telephone extension.
Use Auth ID	This field must be set to Yes.

Auth ID	Use this format: sip:ext@NBX IP address For example: sip:1022@192.168.123.21

7 When you apply these settings, the telephone typically reboots. It then registers itself with the system and is a member of the Telephones list (click T*elephone Configuration* > *Telephones)*. You will have a dialtone and be ready to make and receive calls.

Adding a 3Com 3108 Wireless Telephone

A SIP-mode system supports the 3Com 3108 Wireless Telephone, which uses standard SIP.

The process to add a 3108 Wireless Telephone is similar to adding a generic SIP telephone with the extra step of establishing connectivity between the 3108 and your wireless network.

Follow these steps to add a 3108 Wireless Telephone to your SIP mode system:

1 Log in to the NBX NetSet utility using the administrator login ID and password.

2 Click *User Configuration* > *Users* > *Add.*

Specify an unused extension number, a first name and last name of the user, and select `Default 3108 Wireless Group` as the Telephone Group.

3 Click *OK* to save the new user profile.

4 Configure connectivity settings on the telephone.

The *3108 Wireless Telephone Guide* (click *Downloads* > *Documentation* > *Telephone Guides)* includes complete instructions about how to configure the telephone to connect to a wireless network and to the system.

After you configure the settings on the telephone:

- The telephone sends a registration request that contains the user extension and password information to the system.
- The system validates the telephone user.

  If the data is valid, the system registers the telephone with the IP address information in the registration request. After a successful registration, the new telephone is a member of the Telephones list (click T*elephone Configuration* > *Telephones)*.

11 DIAL PLAN

This chapter provides information about understanding, developing, and managing the dial plan. It describes these topics:

For more information about these topics and configuration procedures, see the online Help.

For general information about Virtual Tie Lines (VTLs) and how to configure them in the dial plan, see "Virtual Connections" on page 329.

Dial Plan Concepts and Overview

The system's dial plan determines how the system manages calls. It defines the set of destinations that the system can reach, how to get to

these destinations, and which telephone numbers to dial to reach these destinations.

The dial plan configuration file is an ASCII text file that implements the dial plan and specifies pretranslation (digit manipulation). The system is shipped with several default dial plan configuration files, typically, a 3-digit and a 4-digit file for each supported country.

The dial plan configuration file includes several tables:

- **Internal** — Must be table ID 1
- **Incoming** — Must be table ID 2
- **Least Cost Routing** — Must be table ID 3
- **Routes**
- **Pretranslators**

You can create additional tables if necessary.

Each dial plan table consists of a series of entries, each of which includes a sequence of digits and the action the system performs in response to sending or receiving those digits. For more information about the Internal, Incoming, and Least Cost Routing dial plan tables, see "Dial Plan Tables" on page 263.

You can access the dial plan configuration file and manage dial plan operations, tables, pretranslators, and extension lists through the NBX NetSet administration utility. However, if your dial plan is larger than 32,000 characters, you cannot use the NBX NetSet utility to edit it. You must export the dial plan, edit it, and then import it.

Before you configure the dial plan, make sure that you understand these concepts:

- Call Process Flow on page 259
- Inbound and Outbound Call Processing on page 259
- System Database on page 260
- System Dial Plan on page 260
- Pretranslation on page 261
- Routing on page 261
- System Features Affected by the Dial Plan Configuration on page 262.

Call Process Flow

The dial plan configuration file is a key component of inbound and outbound call processing. The dial plan tables in the configuration file process *incoming* calls in this order:

1. Incoming Dial Plan Table
2. Pretranslator Table

The dial plan tables process *outgoing* calls in this order:

1. Internal Dial Plan Table
2. Least Cost Routing Table

After pretranslation (if performed), the final translation process routes the call to the destination.

Inbound and Outbound Call Processing

The system routes all inbound and outbound calls through the dial plan.

Inbound Call Processing

The system uses the *Incoming* table to process inbound calls. The system can also use *pretranslators* to perform digit manipulations on incoming calls before it uses the Incoming table.

Each pretranslator operation performs a digit manipulation operation on the dialed digits. For incoming calls, if the DID/DDI (Direct Inward Dial/Direct Dial Inward) range matches the internal extensions, the dial plan requires no pretranslator. However, you can use pretranslators to map nonmatching dialed numbers on an incoming DID/DDI channel to desired internal extensions. See the example in Customer Requirement 1 in "Sample Solutions Using Dial Plan Configuration File Commands" on page 320.

Outbound Call Processing

The system processes outbound calls using the *Internal* dial plan table or the *Least Cost Routing* table. You can add entries to the Internal dial plan table to match the system to your service. See Customer Requirement 2 in "Sample Solutions Using Dial Plan Configuration File Commands" on page 320.

If you have entries in both the Least Cost and Internal tables for the same purpose, the behavior of the dial plan can be confusing. 3Com recommends that you accomplish least cost routing using Internal Table

entries. For more information, see TimedRoute Create, TimedRouteEntry Create, and TimedRouteOperation Create later in this chapter.

System Database

The system database contains a default dial plan that is loaded initially at the factory and is reloaded if you purge the database.

- V3000, V3001R, and V5000 systems — default 4-digit plan
- NBX 100 — default 3-digit plan

The system stores changes that you make to any system settings in the database, which includes changes made when you import a modified dial plan configuration file. When you reboot the system, it loads the database with any changes that you have made. The system database includes the settings necessary for system operation.

System Dial Plan

You can import a dial plan configuration file to provide the system with a set of operating instructions to manage the telephone system. Alternatively, if you make changes to the currently loaded instructions through the NBX NetSet utility, you can export the dial plan configuration file to save it. You can also edit the configuration file off-system with any ASCII editor to make changes, and then import the modified file. You can easily reuse a given configuration file on many systems. For more information, see "Importing and Exporting Dial Plan Configuration Files" on page 275.

The system is shipped with several default dial plan configuration files, typically, a 3-digit and a 4-digit file for each country that is supported. In addition, the `samples.txt` file contains several examples that illustrate how you can configure the dial plan configuration file to control how the system manages incoming and outgoing calls.

Typically, you configure a dial plan completely before you use the system to control the telephones. Although you can make changes later, major changes in the dial plan can disrupt the system.

Decide whether you want to use a 3-digit or 4-digit dial plan before you create the dial plan, autodiscover devices, or manually add telephones or other devices to the system.

When you import a dial plan, some parameters of the system change immediately. Other parameters change only when you reboot the system.

3Com recommends that you reboot the system each time that you change the dial plan.

When you reboot the system, you disrupt service to the telephones. Plan to reboot at a time that does not inconvenience telephone users.

Pretranslation

Pretranslation is the process of translating (or manipulating) dialed digits before they are passed to the appropriate dial plan table for subsequent routing. You can set the dial plan to perform pretranslation on incoming or outgoing calls. For more information, see "Dial Plan Pretranslators" on page 270.

Routing

Routing specifies how a call reaches a destination. You define the routes for the system to use in the Routes section of the dial plan configuration file.

*When you define call routing, you can also instruct the system to perform pretranslations. Both destination routes and timed routes have digit manipulation operations (*append, prepend, replace, stripLead, *or* stripTrail*).*

The system passes dialed digits first through the device's Least Cost Routing table (if there is one). If the system finds no entry, it then uses the Normal dial plan table. If the system does find an entry in the Least Cost Routing table, it attempts to use that entry and, even if the attempt is unsuccessful, it does *not* use the Normal table.

You can route incoming calls to the Auto Attendant port, and you can instruct the Auto Attendant to route these calls to any internal or external number.

CAUTION: *If you configure the Auto Attendant so that it can access any external number, you risk the possibility of toll fraud. To reduce the possibility of toll fraud, include specific external numbers in the outgoing dial plan table. This precaution prevents outside callers from dialing any external number except the ones that you define.*

There are two types of routes:

- **Destination routes** — Specify the extension of a destination device. They can also perform digit manipulation operations on the dialed digits that resulted in the selection of this route before those digits are dialed on the destination device.

- **Timed routes** — Specify time of day and day of week criteria, which when met, result in a particular destination route being selected.

CAUTION: *If you operate the system in Keyset Mode, routes are not applicable.*

For more information, see "DestinationRoute Create" on page 308, "TimedRoute Create" page 316, and related entries under "Dial Plan Configuration File Commands" on page 305.

System Features Affected by the Dial Plan Configuration

The dial plan configuration affects several system features:

- Keyset Mode Operation Using the Dial Plan
- Hybrid Mode Operation Using the Dial Plan
- Off-Site Notification

Keyset Mode Operation Using the Dial Plan

If you map any telephone buttons that have status lights to specific Analog Line Card ports, you enable Keyset mode in the system. Instead of dialing a single digit (typically 8, 9, or 0) before placing an outside call, the telephone user presses a button to select an available Analog Line Card port. The telephone user defines the routing (that is, the selection of a destination device) by pressing the button to select the Analog Line Card port; however the system controls the call using the dial plan.

You cannot map a digital line extension in Keyset mode.

The system applies any Class of Service (CoS) restrictions that are associated with the user's telephone to determine whether to make a call. The system also uses any pretranslator that a device uses and performs any required digit manipulation operations before it transmits the digits on the Analog Line Card or Digital Line Card port.

Hybrid Mode Operation Using the Dial Plan

If you map telephone buttons for some telephones but not others, you enable Hybrid mode (a mixture of standard and Keyset behaviors). The system provides a system-wide External Prefix setting, which allows you to establish a prefix.

Off-Site Notification

The system uses off-site notification to notify telephone users when new voice mail messages arrive. You can define notification devices and assign them in the Internal dial plan as well as through the NBX NetSet utility.

Example: When voice mail arrives, the system dials the telephone number of the telephone user's pager. Typically, you use a system-wide prefix to designate the device or devices you want to use for outdialing purposes, including off-site notification calls.

Example: If the telephone user's pager number is 800-555-3751, and the system-wide prefix digit is 9, the system dials 98005553751 to send a call to the telephone user's pager.

To instruct the system to dial a single Line Card port or a restricted number of Line Card ports, create a suitable pool of Line Card ports for that purpose, and then use an existing set of dial plan table entries (such as the entries that begin with 8) or create a new set of entries to allow the dial plan devices to route calls by means of the selected line card ports.

Example: You set up one 4-port card to manage all off-site notification calls. You create a set of entries in the Internal dial plan table that each start with the digit 8. You define a route to the 4-port card for all of these dial plan entries so that whenever the system acts on one of these entries, it uses one of the 4 ports on that card to dial out and notify the telephone user.

To apply different off-site CoS restrictions to different telephone users, you need multiple dial plan entries. If you are not applying the CoS restrictions, then a single dial plan entry is sufficient.

Dial Plan Tables

Dial plan tables contain information that controls how the system routes calls. Each dial plan configuration file consists of at least three dial plan tables. This section discusses these topics:

- Dial Plan Command Format
- Internal Dial Plan Table — Must be table ID 1
- Incoming Dial Plan Table — Must be table ID 2
- Least Cost Routing Dial Plan Table — Must be table ID 3

- Adding New Dial Plan Tables

CAUTION: *The dial plan must include Tables 1, 2, and 3. Do* **not** *delete them. You may create additional dial plan tables if necessary, but you must number them 4 or higher.*

If the Least Cost Routing table exists, it takes precedence over the Internal table. If the system cannot find a Least Cost Routing table, it attempts to find a corresponding entry in the Internal table. If you have entries for the same purpose in both the Least Cost and Internal tables, the behavior of the dial plan can be confusing.

See "Dial Plan Command Format" next for a description of dial plan command syntax and structure. For a complete list and description of dial plan commands, including command arguments and examples, see "Dial Plan Configuration File Commands" on page 305.

Dial Plan Command Format

Each dial plan table contains a sequence of commands. These commands collectively determine how the system manages calls.

Most of the dial plan commands have a similar format, as shown in Figure 12.

Figure 12 Dial Plan Command Format

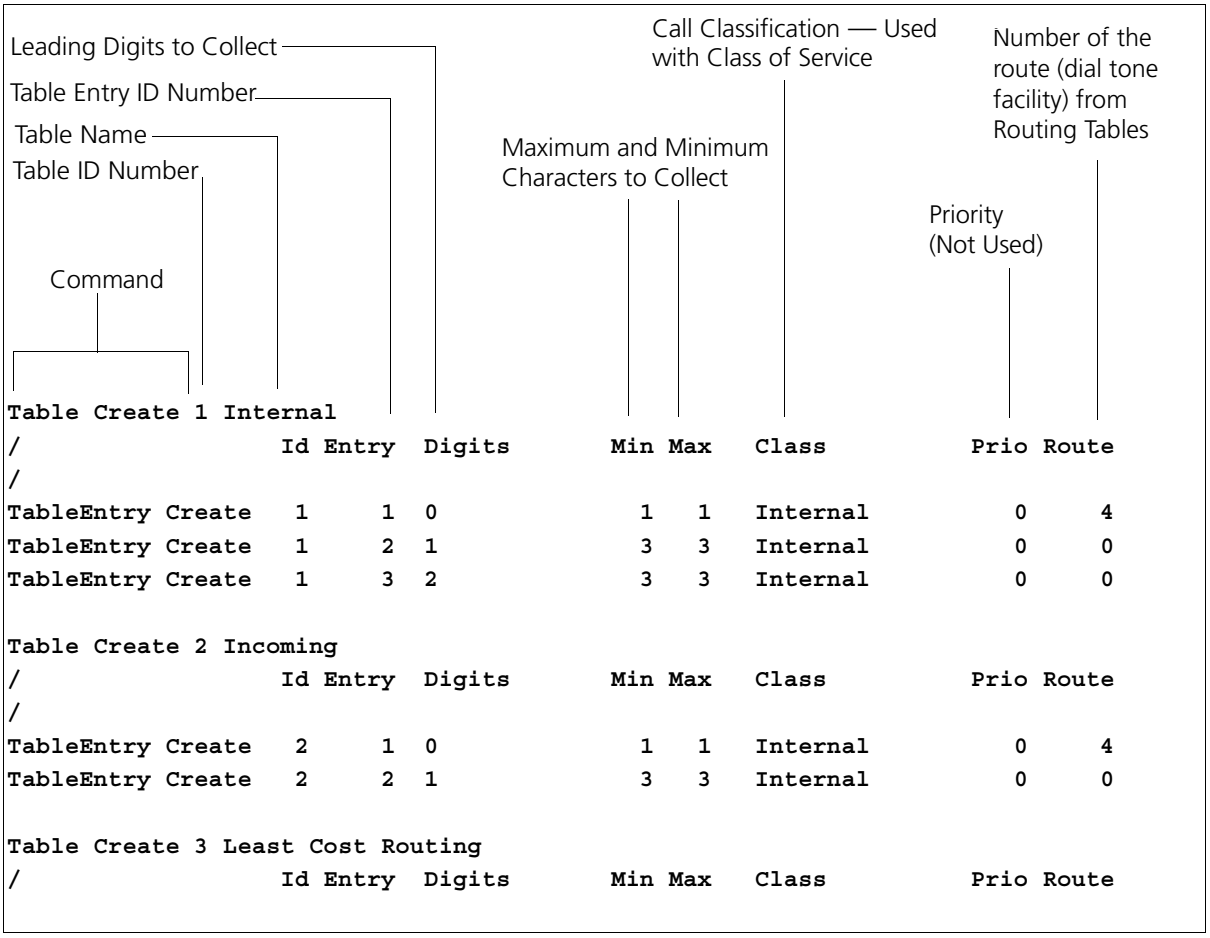


Table 52 describes each field of a dial plan command.

Table 52 Dial Plan Command Fields

Field	Description
Command	Command name. For example, TableEntry Create is the command that makes CoS and call routing decisions based on the correspondence of dialed digits and table entry digits. See "Dial Plan Configuration File Commands" on page 305 for a description of each command.
Table ID Number	Table ID number. This is always 1 for the Internal dial plan table, 2 for the Incoming dial plan table, and 3 for the Least Cost Routing Table.

Table 52 Dial Plan Command Fields (continued)

Field	Description
Table Entry ID Number	Table entry number (a unique number for each entry in the table). Typically, these numbers are in ascending order in the table, but you can change the order. For example, you might want to place a new item near other items of the same type (that begin with the same digit) to help troubleshoot the configuration file.
Digits	One or more digits that begin the dial sequence. Either single or multiple entries can start with the same digit. The system uses this field with the Min and Max fields to determine when to make the call routing decision. Most sample tables have a single entry for digit 0 (zero) to specify how the system manages a telephone number with zero as the first digit. If you want the system to manage calls differently, depending on whether they start with 90 or 91, you must have one entry in the table for each of these 2-digit sequences.
Min	Minimum number of digits that the system collects before routing the call.
Max	Maximum number of digits the system collects before routing a call.
Class	Class of Service (CoS). The system uses this information to determine whether a caller is allowed to make this specific type of call. The possible classifications are: Internal, Local, LongDistance, International, WAN, Toll- Free, Emergency, COCode, Wireless, Toll, Operator, AlternateLong, TrunkToTrunk, Diagnostics, NotAllowed, Other Each of these values corresponds to a selection in the NBX NetSet utility.
Priority	Priority number. This field is not used at this time, but must be present and must always be 0 (zero).
Route	Route number. This identifies an entry in the Routes section of the dial plan. Zero is a typical value for internal calls, and indicates that this call uses no route, in which case, the system transmits the digits as soon as the caller dials them.

If a new entry in the Internal table does not work, it is possible that the system is using an entry from the Least Cost table instead. To avoid such conflicts, you can achieve least cost routing using only the Internal table. To keep the dial plan as simple as possible, 3Com strongly recommends that, you use only the Internal table for least cost routing.

For more information about how to use the dial plan configuration file, see "Managing the Dial Plan Configuration File" on page 273.

Basic Dial Plan Table Examples

These examples describe the basic operation of a dial plan table.

Example: If you use a 4-digit dial plan and the telephone extensions start with 2, then the table entry with 2 in the *Digits* column typically has 4 in the *Min* column. Before making a determination, the system collects all 4

digits of the extension. If the caller dials fewer than the Min number of digits, the system times out in 20 seconds.

Example: If Digits = 2, Min = 4, and Max = 4, the system knows that if the first digit is 2, it must collect no less than 4 and no more than 4 digits before making the call routing decision.

If the caller dials at least the minimum number of digits and not more than the maximum number of digits, the system waits 5 seconds and then routes the call based on the digits the caller dialed. If the caller dials more than the maximum number of digits, the system attempts to place the call.

Often, the Max and Min values are identical, because you want the system to collect a specific number of digits, no more and no less.

Example: For internal extensions, you want the system to collect exactly 3 digits (4 in a 4-digit dial plan) before it makes a determination. Set both Min and Max to 3 (4 in a 4-digit dial plan).

The two columns might be different if the table entry applies to more than one situation.

Example: In the United States, the Min value for the 90 entry is 2, because 90 allows an internal caller to reach a telephone company operator (9 to get an outside line, and then 0 to get the operator). The Max value is 64, because the caller can continue to dial after the zero, enter a number to call, plus a telephone credit card number, and possibly an identification code number.

If the caller dials only 90 (which satisfies the minimum of two digits) and stops dialing, the system waits for 5 seconds. If the caller does not dial other digits, the system connects the caller to the operator.

If the caller dials other digits, the system accepts them up to the limit of 64. If the caller stops after dialing fewer than 64 digits, the system again waits 5 seconds before it acts on the dialed sequence of digits.

Example: You can assign a new employee to the *Default User Group*. You can then set the permissions for that group so that group members have permission to make *LongDistance* calls when the system mode is Open or Lunch, but not when the system mode is Closed or Other.

Example: You can assign the company's Vice President of Finance to a group that you name the *All Privileges Group*. You can set the permissions for that group so that group members have permission to make *LongDistance* calls during all system modes.

Internal Dial Plan Table

The Internal dial plan table (table ID 1) defines how to manage calls placed from internal devices, such as 3Com Business or Basic Telephones, to a destination. A destination can be another internal device, such as a local telephone, or an external telephone line (Analog Line Card or Digital Line Card) that connects the system to other facilities.

The Internal dial plan table consists of a series of commands. For an example of the command format, see "Dial Plan Command Format" on page 264. Table 52 on page 265 describes each element of the command. Table 53 describes the predefined routes.

Table 53 Predefined Routes

Route Number	Description
1	Local CO (strip)
2	Local CO (no strip)
3	Voice Application (Auto Attendant on extension 500)
4	Attendant (person)
5	H.323 Gateway
6	Least Cost Route example
Other	User-defined routes

You cannot delete or modify predefined routes. You can only create new routes.

Each device must have a Normal table. The Least Cost Routing table is optional. Telephones use the Internal dial plan table (table ID 1) as their normal outbound table and the Least Cost Routing table (table ID 3) as their long distance routing table.

Incoming Dial Plan Table

The Incoming dial plan table (table ID 2) defines how the system routes calls, which arrive from outside the system, to extensions. Incoming calls can arrive on analog telephone lines or through Digital Line Card ports.

The incoming dial plan table consists of a series of commands. For an example and basic understanding of the command format, see "Dial Plan Command Format" on page 264. For a description of the each element of a dial plan command, see Table 52 on page 265.

By default, Line Card ports, Digital Line Card ports, and H.323 gateways use the Incoming dial plan table as their normal dial plan table. An Incoming dial plan table typically has a more restricted list of dialable digits than the Internal dial plan table. You usually cannot dial extensions associated with internal paging or Analog or Digital Line Card ports.

Least Cost Routing Dial Plan Table

The Least Cost Routing table (table ID 3) defines how to route calls to minimize the cost of those calls.

Example: You might use two different long distance carriers, one for a specific geographic region, and one for all other areas of the country. In the Least Cost Routing table, you can create entries that route calls differently for those two geographic areas. Each country uses a different method to accomplish this. In the United States, you can specify the area codes that apply to a geographic region. In France, you can specify a carrier by adding prefix digits to the telephone number.

By default, internal telephones specify the Least Cost Routing table as their least cost table. Typically, devices associated with the Incoming dial plan table (Line Card ports, Digital Line Card ports, and H.323 gateways) do not use the Least Cost Routing table.

The Least Cost Routing table is optional. If it does not exist, the system uses the Internal table routing destinations. If you have entries in both the Least Cost and Internal tables for the same purpose, the behavior of the dial plan can be confusing. Therefore, 3Com recommends that you accomplish least cost routing using Internal Table entries. See TimedRoute Create, TimedRouteEntry Create, and TimedRouteOperation Create.

Example: If a new entry in the Internal table does not work, it is possible that the system is using an entry from the Least Cost table instead. To avoid such conflicts, you can achieve least cost routing using only the Internal table. To keep the dial plan as simple as possible, 3Com strongly recommends that, you use only the Internal table for least cost routing.

Adding New Dial Plan Tables

If you share the system with another company or group and want to control calls differently at the two sites, you can add a fourth table.

Example: Assign one extension range to Company A and a different range to Company B. The fourth table controls the extension range for Company B, so that outbound calls from Company B's extensions use only their external telephone lines.

You might need a fourth table if a company has two sites but only one system. To route emergency (911) calls properly, use the fourth table to define which extensions use each dedicated 911 telephone line.

Example: Telephone users at Site A dial 911 and the system uses the Internal table (table ID 1) to make the emergency call on one external telephone line. Users at Site B dial 911 and the system uses table ID 4 to make the emergency call on a different external telephone line. The emergency staff know, based on the dialing number, which site has the emergency.

Enhanced 911, E911, is available in some areas. This service enables emergency staff to identify the specific location of the emergency. For example, in a campus of buildings, the emergency staff can identify the specific building, floor, and location from which the emergency call originates. The system supports E911 over ISDN. You must define an outbound call pretranslator to provide the specific extension number from which the 911 call originates.

Dial Plan Pretranslators

The system uses pretranslators to modify digit sequences of incoming or outgoing calls. On incoming calls, pretranslators can map the entire dialed number (including area code) to an internal extension number. For example, an external caller dials 978-555-0101 to reach the person on extension 101. Pretranslators ensure that the proper digits are mapped to the correct extension number.

For more information, see:

- Pretranslators for Incoming Calls on page 271
- Pretranslators for Certain Outgoing Calls on page 272

A typical pretranslator function involves mapping incoming DDI/DID telephone calls to internal extension numbers.

Example: The DDI/DID telephone numbers range from 508-555-4200 through 508-555-4299. The telephone company sends you the last

4 digits of the total telephone number. Internally, you want to use extensions 2000 through 2099. You can define a pretranslator to:

- Remove (stripLead) the first two digits of the incoming 4-digit sequence.
- Add (prepend) the digits 20 in front of the remaining 2 digits.

See "Managing Dial Plan Pretranslators" on page 296 for detailed information about and examples of how to create and manage dial plan pretranslators.

Pretranslators for Incoming Calls

For incoming calls, pretranslation reformats the dialed number *before* it is passed to the Incoming dial plan table (Table ID 2). See "Incoming Dial Plan Table" on page 268. For information about how to manage caller ID and CDR information for incoming VTL calls, see "Creating a Pretranslator for VTL Calls" on page 297.

Incoming Pretranslator Example 1

For an incoming telephone call, if the telephone company passes you 4-digit numbers from 6100 through 6199, the system can use a pretranslator to remove the first digit; the remaining 3 digits can then be used as internal extension numbers in a 3-digit dial plan. Define digit manipulation operations (*append, prepend, replace, stripLead,* or *stripTrail*) within the *PreTranslator section* of the dial plan configuration file to indicate which pretranslations you want to perform.

Incoming Pretranslator Example 2

Assume the telephone company passes 10-digit numbers to the system for each incoming telephone call (for example, numbers in the range 4567-89-3000 to 4567-89-3500). If the system uses 4-digit extensions in the range 2000 to 2500, you could pass an incoming 10-digit number such as 4567-89-3210 to extension 2210.

This strategy requires two pretranslation operations: The first operation performs a *stripLead* operation to remove the initial 7 digits, leaving 210. The second operation *prepends* the number 2 in front of the remaining 3 digits. The result is 2210, which matches an extension within the extension range. "Sample Solutions Using Dial Plan Configuration File Commands" on page 320 shows how to accomplish this pretranslation using the dial plan configuration file.

Each device can specify only one DDI/DID pretranslator and one Calling Line ID Presentation (CLIP) pretranslator. To create or modify a pretranslator, you either edit a dial plan configuration file and import it, or use the NBX NetSet utility and modify an existing dial plan configuration file.

The system performs operations in ascending order of operation ID. Operations are both sequential and cumulative.

You can also use pretranslators with virtual tie lines to link multiple systems. Incoming calls within a defined numeric range arrive at the first system, are modified through digit manipulation operations, and are then routed to a tie line connected to a second system.

Each sample dial plan that is shipped with the system includes a default pretranslator.

Pretranslator Example 3

Assume that the telephone company passes 4-digit numbers to the system for each incoming telephone call (for example, numbers in the range 5200 through 5300). If the system uses 3-digit extensions in the range 200 through 300, you could define a single pretranslation operation to *stripLead* (remove) the first digit, for instance, the number 5 from an incoming number such as 5278, and pass the call to extension 278. "Sample Solutions Using Dial Plan Configuration File Commands" on page 320 shows how to accomplish this pretranslation using the dial plan configuration file.

Pretranslators for Certain Outgoing Calls

On outgoing calls using an ISDN PRI card, pretranslators allow the external called party to identify the full number of the internal caller, including the area code. For example, if the person on extension 101 within a company calls an external number, the caller's entire number is displayed to the called party when CLIP pretranslators are used. Pretranslation reformats the outgoing dialed number *before* it is passed to the Internal dial plan table (Table ID 1) or possibly the Least Cost Routing table (Table ID 3). For more information, see "Internal Dial Plan Table" on page 268 and "Least Cost Routing Dial Plan Table" on page 269.

Example: If the DDI/DID telephone numbers range from 508-555-4200 through 508-555-4299, internally, you dial extensions from 2000 through 2099 to reach another internal telephone.

When you place a call to an external telephone number, the system can use these pretranslator steps to create the full 10-digit number:

1. Remove (stripLead) the first two digits (20) from the internal extension number of the telephone making the call.
2. Add (prepend) the digit sequence 50855542 to the two remaining digits, creating the full DDI/DID telephone number.
3. Pass the full number to the telephone company.

Example: To transmit CLIP information about outgoing calls, you can define a pretranslator that transforms internal extensions into full telephone numbers (the numbers that someone external to the company uses to dial in). Assume that you use telephone extension numbers from 1000 to 1099 and that only the last two digits match the DDI/DID numbers that are assigned to the company. You can define a pretranslator to remove *(stripLead)* the first two digits from the internal extension number and add (*prepend*) the appropriate digit string. This pretranslator constructs the full telephone number.

Example: If you use two different long-distance carriers at different times of the day to save costs, you can prepend different digit sequences to the outgoing dialed number to select which carrier that you want. If you prepend 1010321 between the time the business opens and 3:00 p.m., you select one long-distance carrier. If you prepend 1010220 from 3:00 p.m. until the next time the business opens (including weekends), you select the other carrier and obtain a lower rate.

Define digit manipulation operations (*append, prepend, replace, stripLead,* or *stripTrail*) in the Routes section of the dial plan configuration file to indicate which outgoing pretranslations you want to perform. You can define these commands for both destination routes and timed routes. For more information about how to configure pretranslators, see "Managing Dial Plan Pretranslators" on page 296.

Managing the Dial Plan Configuration File

This section describes the dial plan configuration file and how to manage it. From the *Operations* tab of the Dial Plan window, you can perform these tasks:

- Accessing the Dial Plan
- Creating Dial Plan Configuration Files
- Importing and Exporting Dial Plan Configuration Files

Accessing the Dial Plan

To import a dial plan configuration file and modify it, log in to NetSet and click *Dial Plan* > *Configure*, which displays the Operations window. From this window, you can access customer-defined and default dial plans.

Creating Dial Plan Configuration Files

The simplest way to create a new dial plan is to model it after an existing one.

1. Log on to NetSet using the administrator login ID and password.
2. Click *Dial Plan* > *Configure*.
3. Browse for a dial plan, or select one from the pull-down list.
4. Click *Open* to open the file in your browser.
5. Click *Save As* and save the dial plan as a new file.

You can now edit the file with an ASCII editor. After you customize the new dial plan, Import it to the system. see "Importing and Exporting Dial Plan Configuration Files" on page 275.

3Com recommends that you enter these commands at the top of every dial plan configuration file:

```
Table Delete *
DestinationRoute Delete *
TimedRoute Delete *
PreTranslator Delete *
```

When you subsequently import this dial plan, these commands purge any traces of the old dial plan and prevent any conflicts that can result from importing one dial plan on top of an existing one.

You create new entries in the dial plan configuration file by typing in new commands (see "Dial Plan Configuration File Commands" on page 305) or by cutting, pasting, and editing existing lines in the file.

When you cut and paste new lines into dial plan tables, make sure you change the Entry number in the pasted line. If two or more lines have the same Entry number, only the last one takes effect.

Importing and Exporting Dial Plan Configuration Files

You import a dial plan configuration file either to implement changes you made by editing the file, or to reload a previously saved configuration.

From the *Operations* tab of the Dial Plan window, you can:

- Import a North American Dial Plan
- Import an International Dial Plan

When you export the working dial plan, the system constructs a *new* configuration file from the values in the database and displays it. The new file shows the current date and time. You name the file when you save it.

The sample, default files include examples of timed routes and pretranslators. To preserve the default (sample) dial plan configuration included with the system, 3Com advises you to choose a unique file name for new files so that you do not overwrite the sample default files.

Import a North American Dial Plan

The default dial plan scheme is as follows:

- V3000, V3001R, and V5000 system — `NorthAmerica-4-digit.txt`
- NBX 100 system — `NorthAmerica.txt`

The system includes customized dial plans for use in other countries.

Always read the system Release Notes (`readme.txt`) for the most up-to-date information about dial plans.

To import a default dial plan configuration file:

1. Click *Dial Plan* > *Configure*.
2. Click the *Default File* radio button and from the Default File drop-down list, select the default file that you want to use.
3. Click *Import*.

CAUTION: *When you import a dial plan configuration file, the system immediately implements the dial plan. You are warned that the system might become inoperative. The system becomes inoperative* only if *you have modified a dial plan manually and have made syntax or content*

errors. Carefully check any changes that you make to the configuration file before you import it.

4 Click *OK*. The system imports the new dial plan and produces a report of any errors.

5 Reboot the system.

Import an International Dial Plan

To change the default North American dial plan to a country-specific dial plan:

1 Click *Dial Plan* > *Configure*.

2 Click the *Default File* radio button and from the Default File drop-down list, select the country-specific file that you want to use.

3 Click *Import*.

CAUTION: *When you import a dial plan configuration file, the system immediately implements the dial plan. You are warned that the system might become inoperative. The system becomes inoperative* only if *you have modified a dial plan manually and have made syntax or content errors. Carefully check any changes that you make to the configuration file before you import it.*

4 Click *OK*. The system imports the new dial plan and produces a report of any errors.

5 Reboot the system.

You might see a warning that "destination extension list is empty." This means that a particular type of device is not installed. You may safely ignore this type of warning.

International Dial Plan Issues

Several international dial plan issues require attention:

Customizing an International Dial Plan. If there is no customized dial plan for your country, you might need to modify the default dial plan. See "Modifying a Dial Plan Configuration File" on page 281. If you edit the default dial plan, you can test the changes by making a simulated call. See "Testing a Dial Plan" on page 279.

Autodiscovering Internal Telephones. If you autodiscover your company's internal telephones, Auto Discovery usually begins at number 100 or 1000. However, for some countries, internal telephones begin at a

higher number to allow you to dial numbers considered of national importance directly. Auto Discovery allocates telephone extensions numbers within this range:

- The default dial plan for the V3000, V3001R, and V5000 systems allows you to allocate internal telephones to extension numbers 1000 through 3999.
- The default dial plan for the NBX 100 allows you to allocate internal telephones to extension numbers 100 through 449.

For more information about Auto Discovery, see "Auto Discovery" on page 27

Dialing Outside Lines. To obtain an outside line, dial 9 or 0 as appropriate for your country.

WARNING: *You must first obtain an outside line before you can dial emergency numbers.*

Importing a User-Defined Dial Plan

To import a customer-defined (user-defined) dial plan configuration file:

1. Click *Dial Plan* > *Configure*.
2. In the *User-Defined File* field, enter the path and name of the user-defined configuration file, or click *Browse* to find the file that you want.

The system has no predefined location for dial plan configuration files. You can specify any directory or path that you want.

3. Click *Import*

CAUTION: *When you import a dial plan configuration file, the system immediately implements the dial plan. You are warned that the system might become inoperative. The system becomes inoperative* only if *you have modified a dial plan manually and have made syntax or content errors. Carefully check any changes that you make to the configuration file before you import it.*

4. Click *OK*. The system imports the new dial plan and produces a report of any errors.
5. Reboot the system.

Exporting (Saving) a Dial Plan Configuration File

When you export (save) the current configuration, the system creates a new dial plan configuration file from the current database. You save the new text file using a name that you choose.

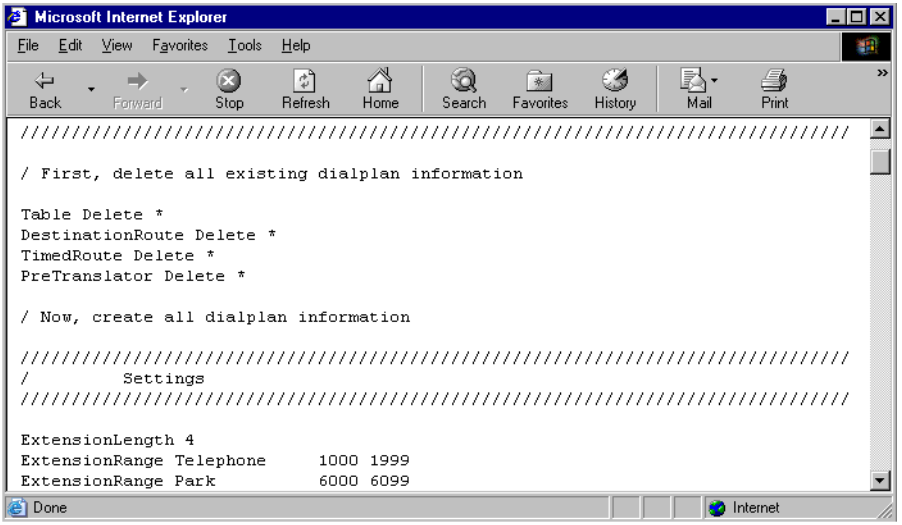
This example refers to Internet Explorer. If you use another browser, you might need to use slightly different procedures.

To export a dial plan configuration file:

1. Click *Dial Plan* > *Configure*.
2. Click *Export*.

   The system constructs a new configuration file from the current values in the database and displays it. Figure 13 shows a partial display. Scroll your browser window to see your complete dial plan.

Figure 13 Dial Plan Configuration File (partial)



3. Click the *File* menu and select *Save As*.
4. From the list box at the top of the *Save As* window, select the destination folder.
5. In the *File Name* field, replace the default file name with a new name.

The sample, default files include examples of timed routes and pretranslators. To preserve the default (sample) dial plan configuration included with the system, 3Com advises you to choose a unique file name for new files so that you do not overwrite the sample default files.

6 Click *Save*.

Testing a Dial Plan

This section describes how you can place a simulated call to test the currently loaded dial plan.

Even if your system is completely installed and operational, a test places a simulated, not an actual call.

Example: If you have an entry in the dial plan for digit sequences that start with 91, with Min and Max set to 5, and you test the sequence 9123, the dial plan test reports an insufficient number of digits. However, in actual operation, the system would time out waiting for the fifth digit, and then attempt to place the call. Assuming that the outside line prefix is 9 (such as in the United States), this situation would obtain an outside line (9) and then dial the numbers 123.

You can specify a day of the week and a time by selecting entries from the *Day/Time* list boxes. This choice instructs the system to act as if the day and time you select are the current day and time.

If you define timed routes in the dial plan, you use different day and time settings to determine whether the timed route works properly.

Example: You can define a timed route to select route 35 during open business hours Monday through Friday, but to select route 36 when business is closed on those days and on weekends. After you define the timed route commands and import the modified file, test using days and times within business hours (to verify that the system selects route 35) and during closed hours and weekends (to verify that it selects route 36).

You can also use day and time settings to test whether the Class of Service settings operate as expected.

Example: You can configure the dial plan to allow toll calls from an extension during open business hours, but to disallow such calls when the business is closed and on weekends. Test using days and times within business hours (to confirm that you can make toll calls from that extension) and during closed hours and weekends (to confirm that the system prevents such calls).

To create and run a test using the currently loaded dial plan:

1. Click *Dial Plan* > *Configure*.
2. Click the Test tab to display the list of extensions from which you can call.
3. Click the extension from which you want to dial for the test.
4. In *Number to dial*, enter the number that you want the system to dial.
5. Select the desired date and time in the *Day/Time* pull-down lists.

For some tests, the day and time settings are irrelevant. You can leave the settings at their default values (Sunday, 00, and 00).

6. Click *Test*. The test runs and the results appear in the dialog box.

Generating a Dial Plan Report

This section describes how to create a report that contains all dial plan settings, tables, routes, and pretranslators. Also, the report:

- Performs a consistency check to ensure that all dial plan table entries point to valid routes which, in turn, point to valid extensions.
- Identifies how many devices are using each dial plan table and each pretranslator.

To generate a dial plan report:

1. Click *Dial Plan* > *Configure*.
2. Click *Reports*, which displays the dial plan report in the browser window.

   Errors can prevent calls from being successfully routed. Warnings are conditions that you can easily correct to route the call successfully.

To record test results and send them to someone, select the text in the results pane and use the browser's copy function (typically found in the Edit menu) to copy the test results to another application window, such as an editor or e-mail.

3. Click *Close*.

The person who validates the dial plan test is responsible for verifying that the test call used the correct dial plan table and dial plan table entry.

Be aware of these common dial plan problems:

- Dial plan table entries that point to nonexistent routes
- Timed route entries that point to nonexistent destination routes

- Destination route entries that point to nonexistent extensions or empty extension lists
- Timed route entries that overlap
- Devices that do not specify a normal table
- Devices that point to nonexistent Normal tables, Least Cost Routing tables, or pretranslators
- Pretranslator entries that have no operations

If a telephone has no table assigned, that telephone does not have permission to dial. The system reports this error. If a device has only a Normal table, the system reports no error.

If a device has only a Least Cost table, the system reports an error. The telephone is still usable and has permissions defined in whatever table has been chosen as Least Cost. If a device has both a Normal and Least Cost table, the system reports no error (the usual condition).

When the system detects an error in any line of an imported dial plan configuration file, it ignores that line and continues to process all remaining lines in the file. This precaution minimizes the impact of errors on the dial plan.

Modifying a Dial Plan Configuration File

This section describes how to modify the currently loaded dial plan configuration file.

CAUTION: *Modifications must be syntactically correct. Each time that the system imports a dial plan configuration file, it verifies the file for errors and displays the results. To avoid typing mistakes, 3Com suggests that you start with an existing dial plan (for example, one of the default plans that are shipped with the* system *or a plan from another system), modify it, and save it as a renamed file.*

To modify a dial plan configuration file:

1. Click *Dial Plan > Configure*.
2. Click the *Modify* tab. Scroll up and down the browser window to see the complete dial plan.
3. Edit the dial plan configuration file.

   A single line of space is *required* between each dial plan entry. You can type a complete dial plan entry anywhere in the file.

4 Click *Apply* and then click *OK* to confirm.

The system imports the modified dial plan and displays the results of the error and consistency checks.

5 To correct any errors, edit the file and click *Apply*. You might be required to make changes based on warning messages.

Outdialing Prefix Settings

A telephone user can use the telephone display panel to look up a call in the call logs (Missed Calls, Answered Calls, and Dialed Calls), select a telephone number from any of the logs, and redial it.

To redial a number from the Missed Calls or Answered Calls list, the system must know the appropriate dial prefix to prepend to the digits in the telephone number.

For information about and examples of how to configure outdialing prefixes, see the online Help.

Managing Extensions

This section describes how to add, change, and manage extensions:

- Extension Settings Overview
- Changing Extension Length and Ranges
- How Auto Discovery Assigns Extensions
- Modifying Extensions
- Converting Extensions

Extension Settings Overview

The system establishes connections between extension numbers. The concept of an extension applies to more than just telephones. Extensions are also assigned to applications such as Call Park zones, Auto Attendants, hunt groups, Line Card ports, voice mail ports, and virtual devices such as the pcXset™ PC soft telephone Client and the ConneXtions H.323 Gateway.

The extension length (either 3 or 4 digits), which applies to all extensions on a system, indicates that all extensions contain that number of digits. You cannot mix 3-digit and 4-digit extensions within the same system. Systems support 3-digit and 4-digit dial plans, although there are some differences in the extension ranges as noted in these tables. By default,

NBX 100 systems use a 3-digit dial plan, and V3000, V3001R, and V5000 systems use a 4-digit dial plan.

Table 54 lists typical extension ranges by type. Table 56 describes these ranges in more detail.

Table 54 Typical Extension Ranges by Type

Extension Type	4-digit
Telephones	1000–3999
Auto Attendant	500, 501, plus 5500–5599
Hunt Group	4000–4099
External Extensions (includes line card ports and Call Park)	6000–7999 (external Auto Discovery starts at 7250)
Call Park (must fall within External Extension range)	6000–6099

Note 1: The V3000, V3001R, and the V5000 systems are shipped with a factory default 4-digit dial plan. If you import any 3-digit plan, you must manually specify any 3-digit extension ranges that are not set by the imported plan. You must also manually change any device extensions so that they fall within the appropriate range.

Note 2: The NBX 100 system is shipped with a factory default 3-digit dial plan. If you import any 4-digit plan, you must manually specify any 4-digit extension ranges that are not set by the imported plan. You must also manually change any device extensions so that they fall within the appropriate range.

Note 3: TAPI Route Point extensions occur in the same range as telephones. TAPI Route Point extensions do not appear in telephone lists within the NBX NetSet utility. For more information about TAPI Route Points, see "TAPI Route Points" on page 351.

Note 4: An extension cannot begin with a zero.

Table 55 Typical Extension Ranges for 3-digit and 4-digit Dial Plans

Extension Type	3-digit	4-digit
Telephones	100–449	1000–3999
Auto Attendant	500–599	500, 501, plus 5500–5599
Hunt Group	450–499	4000–4099
External Extensions (includes line card ports and Call Park)	600–799 (external Auto Discovery starts at 750)	6000–7999 (external Auto Discovery starts at 7250)

Table 55 Typical Extension Ranges for 3-digit and 4-digit Dial Plans (continued)

Extension Type	3-digit	4-digit
Call Park (must fall within External Extension range)	601–609	6000–6099

Note 1: The V3000, V3001R, and V5000 systems are shipped with a factory default 4-digit dial plan. If you import any 3-digit plan, you must manually specify any 3-digit extension ranges that are not set by the imported plan. You must also manually change any device extensions so that they fall within the appropriate range.

Note 2: The NBX 100 system is shipped with a factory default 3-digit dial plan. If you import any 4-digit plan, you must manually specify any 4-digit extension ranges that are not set by the imported plan. You must also manually change any device extensions so that they fall within the appropriate range.

Note 3: TAPI Route Point extensions occur in the same range as telephones. TAPI Route Point extensions do not appear in telephone lists within the NBX NetSet utility. For more information about TAPI Route Points, see "TAPI Route Points" on page 351.

Note 4: An extension cannot begin with a zero.

Table 56 provides a more detailed explanation of extension types, including default extension ranges and values for 3-digit and 4-digit dial plans.

Table 56 Dial Plan Extension Settings

Field	Purpose (See Notes 1 – 3)
Telephone Extensions	The range of extensions for telephones. ■ **4-digit dial plan:** 1000–3999 ■ **3-digit dial plan:** 100–449 TAPI route point extensions are included in the telephone extensions range. *Length* — This drop-down list specifies the number of digits for telephone extensions. **Note: An extension cannot begin with a zero.**
Auto Attendant Extensions	The range of extensions for Auto Attendants. Default: ■ **4-digit dial plan:** 5500–5599 ■ **3-digit dial plan:** 500–599 For both 3-digit and 4-digit dial plans: ■ Extension 500 is reserved as the default Auto Attendant. ■ Extension 501 is reserved as the voice mail Auto Attendant.

Table 56 Dial Plan Extension Settings (continued)

Field	Purpose (See Notes 1 – 3)
Default Auto Attendant Extensions	Default extension that the system assigns to the default Auto Attendant. The Auto Discovery process assigns this extension. The system must direct each call coming in on an external line to an extension. During the Auto Discovery of external lines (analog lines and Digital Line Card channels), the system assigns the default extension (500) as the Auto Attendant extension. After you import the dial plan configuration file and complete the Auto Discovery process, you can manually configure the extension for each analog line and each Digital Line Card channel. For both 3-digit and 4-digit dial plans: ■ Extension 500 is reserved as the default Auto Attendant. ■ Extension 501 is reserved as the voice mail Auto Attendant.
Hunt Group Extensions	The range of extensions for hunt groups. ■ **4-digit dial plan:** 4000–4099 ■ **3-digit dial plan:** 450–499
External Extensions	The range of extensions that are connected to external devices, such as Analog Line Card ports, Digital Line Card ports (BRI-S/T, T1, E1, ISDN PRI), Call Park, and Paging extensions. Default: ■ **4-digit dial plan:** 6000–7999 ■ **3-digit dial plan:** 600–799
Call Park Extensions Range	The range of extensions for Call Park. This feature allows the telephone user to park a telephone call temporarily and then pick it up at a different telephone. Call Park extensions must be a subset of *external* extensions. ■ **4-digit dial plan:** 6000–7999 ■ **3-digit dial plan:** 600–799
Start External Discovery At	The system assigns extensions to external devices it autodiscovers, starting with this number and incrementing upward. If the system reaches the highest extension, it starts searching from the beginning of the external range and selects the first unused one. Typically, systems do not use all of the available external extensions from 600–799 in a 3-digit dial plan or from 6000–7999 in a 4-digit dial plan. Default: ■ **4-digit dial plan:** 7250 ■ **3-digit dial plan:** 750

Table 56 Dial Plan Extension Settings (continued)

Field	Purpose (See Notes 1 – 3)
External Keyset Prefix	In Keyset mode, when a button on a 3Com Business Telephone directly accesses an outside line, the system must check Class of Service. The system prepends the *External Keyset Prefix* value (typically 8, 9, or 0) when it makes a call in Keyset mode.
Default Auto Extension	Default extension that the system assigns to the default Auto Attendant. The Auto Discovery process assigns this extension. Default menu Auto Attendant: 500 Voice mail Auto Attendant: 501

Note 1: The V3000, V3001R, and V5000 systems are shipped with a factory default 4-digit dial plan. If you import any 3-digit plan, you must manually specify any 3-digit extension ranges that are not set by the imported plan. You must also manually change any device extensions so that they fall within the appropriate range.

Note 2: The NBX 100 system is shipped with a factory default 3-digit dial plan. If you import any 4-digit plan, you must manually specify any 4-digit extension ranges that are not set by the imported plan. You must also manually change any device extensions so that they fall within the appropriate range.

Some countries reserve numbers that begin with 11 for numbers of national importance. To accommodate this requirement, you can begin the telephone extension range at 120.

Changing Extension Length and Ranges

You can view and change extension settings, such as extension length and extension ranges.

If you change from a 3-digit to a 4-digit plan, import the 4-digit dial plan configuration file before *you configure or autodiscover any devices.*

To view and change extension settings:

1. Click *Dial Plan* > *Configure*.
2. Click the Settings tab.
3. Make the desired changes to the extension settings. Table 56 describes each field.
4. Click *Apply*.

Planning Extension Ranges

Plan extension ranges to accommodate your present and future needs. An extension cannot begin with a zero.

Example: If you initially have 60 telephones and expect to add no more than 100 additional telephones in the future, choose 100–299 as the telephone extension range (1000–1199 in a 4-digit system). This arrangement provides 200 extension numbers to manage the planned 160 telephones plus 40 extra extensions to manage unexpected additions.

Once you set the telephone extension range, you can extend it later, provided that the new range does not overlap any other number range.

Example: For a 4-digit dial plan, you can set the initial telephone extension range to 1000–1099. This arrangement allows for up to 100 telephone extensions. Later, you can extend the range up to 3999 to allow for 400 telephone extensions. By default, the Hunt Group range starts at 4000, 450 for a 3-digit dial plan, so you cannot assign telephone extensions in either of those ranges.

How Auto Discovery Assigns Extensions

The Auto Discovery process assigns new extensions to telephones and other devices. For example, if you install a T1 or E1 Digital Line Card, you can use Auto Discovery to assign extension numbers to each port on the card. The Auto Discovery process initially assigns a default name *(new user)* to each new telephone, and assigns the next available extension number. Later, you can replace *(new user)* with the appropriate telephone user's name.

It is possible to bypass the Auto Discovery process and to add a new telephone and assign an extension manually. However, 3Com strongly recommends that you take advantage of the Auto Discovery process. For instructions about how to use Auto Discovery, see *"Adding a New Telephone" on page 93*.

You can define a telephone user in the system database and not assign a telephone to that user. When you define a telephone user with only a telephone extension, you create a *phantom mailbox*. The system associates an extension with this phantom mailbox so that the telephone user has voice mail capability. To access voice mail from any telephone, the telephone user calls either extension 500 (the default Auto Attendant extension), or 501 (the default Auto Attendant voice mail extension.)

Telephones and Line Card ports reserve most of the extensions within the system. However, there are other extensions within the system. Table 54 lists the default extension ranges for 3-digit and 4-digit dial plans.

Modifying Extensions

You can modify the extension number of any device in the system. Normally, you make changes *only* after you have changed the extension ranges for the system, to align the extensions with the new ranges.

CAUTION: *Be careful when you change extensions. The system does not validate changes that you make, and there is no* Undo *or* Cancel *function. A mistake can compromise the operation of the system.*

To modify extensions:

1. Click *Dial Plan* > *Configure*.
2. Click the Modify Extensions tab.
3. Select the extension, or extensions, that you want to modify. To select all extensions, enable the *Select* check box.
4. Select an operation from the drop-down list and make the appropriate entries in the field, which display after the member list:
   - **Change Extension** — Modifies the first selected extension with the number you type in the field next to the drop-down list. Change Extension applies to only one extension at a time. If you select multiple extensions, the system changes only the first extension that you selected.
   - **Prepend** — Prepends digits in front of all selected extensions.
   - **Append** — Appends digits to the end of all selected extensions.
   - **Strip Leading Digit**s — Strips (removes) the specified number of digits from the beginning of all selected extensions. For example, if you type the number 2 in the field, the system strips (removes) two digits from the beginning of the extension.
   - **Strip Trailing Digit**s — Strips (removes) the specified number of digits from the end of all selected extensions.Click *Apply* to make the changes, or click *Reset* to restore the settings to their original status.

If the requested change creates a duplicate extension or an extension of zero length, the system discards the change. For example, if you select extensions 1000 through 1009 and select *Strip Trailing Digits*, the system makes no change, because the result is a series of identical numbers (all 100).

Converting Extensions

The Convert Extensions feature enables you to use the NBX NetSet utility to change these extension types from 3-digits to 4-digits or from 4-digits to 3-digits quickly:

- Virtual Tie Line (VTL) extensions
- Voice mail port extensions
- Call Park extensions
- Paging extensions

The Convert Extensions feature helps you in the larger task of converting a dial plan between 3- and 4-digits. To perform a complete a dial plan conversion, you must also manually convert any existing extensions for these extension types:

- External extensions (Analog Line Card ports, Analog Terminal Card ports, and Digital Line Card channels extensions)
- Internal extensions, which includes TAPI Route Point extensions
- H323 Gateway extensions
- Hunt Group and Automatic Call Distribution Group extensions

To convert a dial plan between 3- and 4-digits, follow these steps:

1 If the conversion is part of a hardware upgrade:

a Install the new hardware.

b Install new licenses on the new system. You cannot move licenses from the old system to the new system. Licenses keys are tied to a system (hardware) ID number.

2 If you are upgrading your hardware, migrate your data from the old system to the new system. For details about data migration, see "Migrating Data" on page 88.

3 Click *Dial Plan* > *Configure.*

4 Make sure the system is set up for the type of dial plan you want. For example, if you are converting an existing system from a 3-digit to a 4-digit dial plan, import the 4-digit dial plan. The 4-digit dial plan is the default dial plan for V3000, V3001R, and V5000 systems.

5 Click *Convert Extensions*.

The system automatically converts existing extensions of these extensions to conform with the dial plan (3-digit or 4-digit) that is currently installed on the system:

- Call Park extensions
- Voice mail port extensions

- Virtual Tie Lines
- Paging extensions

6 Manually specify new values for any of these existing extensions:

- Telephone Extensions
- Auto Attendant Extensions
- Hunt Group and ACD Group Extensions
- External Extensions (digital channel and analog port extensions)

To modify an existing extension, click *Dial Plan > Configure,* and then click the Modify Extensions tab. Edit the list of extensions so that each extension falls into the range for its extension type:

Extension Type	3-digit Dial Plan Defaults	4-digit Dial Plan Defaults
Internal Extensions	100-449	1000-3999
Hunt Group and ACD Group Extensions	450-499	4000-4099
Auto Attendant Extensions	500-599	5500-5599
External (digital and analog line card port) extensions	600-799	6000-7999
	The external extension range includes Call park extensions, which are converted when you use the Convert Extensions feature described previously in step 4.	

7 Edit your dial plan to configure any needed modifications such as pretranslators.

Managing Extension Lists

An extension list contains extension numbers that you assign and dedicate to specific dial tone facilities or to specific applications (voice mail, Auto Attendant, and so on), or both. You can add an extension list to define a subset of devices, such as fax machines.

The system default extension lists are numbered starting at *0001 in either a 3-digit or 4-digit plan. By convention, a default extension list number is preceded by an asterisk. See Table 57 for a description of the standard extension lists.

CAUTION: *Extension lists must not overlap.*

Table 57 Extension Lists

Extension List ID	Description
*0001	Contains extension numbers assigned to Analog Line Card ports. Routes 1 and 2 use this list.
*0002	Contains extension numbers assigned to Digital Line Card ports. Routes 1 and 2 use this list.
*0003	Contains extension numbers assigned to voice mail. ■ **4-digit dial plan:** 6400–6499 ■ **3-digit dial plan:** 651-662 Route 3 uses this list.
*0004	Contains the extension for the attendant (that is, the person who monitors incoming calls). The system automatically assigns the lowest extension found during Auto Discovery to this list. Route 4 uses this list.
*0005	Contains extension numbers assigned to H.323 ports.
*0006	Contains extension numbers assigned to Virtual Tie Lines (VTL).
*0008	Contains extension numbers assigned to the 8-pool.

Within an extension list, you can assign a priority to each extension. When the system accesses an extension list, it tries to use the highest priority extension first. The highest priority is 1 and the lowest is 99.

For example, if the extension list contains extensions that you assigned to T1 channels, you can assign unique priorities to each of the extensions. If you instruct the system to place an outgoing call using the T1 line, it attempts to use the highest priority extension/channel first. If the first is unavailable, it tries the next highest priority extension/channel, and so on.

From the *Extensions List* window, you can perform these tasks:

- Adding an Extension List
- Modifying an Extension List
- Removing an Extension List

The system restricts access to any specific Analog Line Card port or Digital Line Card port. To dial the extension number that is associated with one of these devices directly, you must have diagnostic privileges. In addition, you cannot dial a prefix to obtain a Digital Line Card port.

Adding an Extension List

To add a new extension list:

1. Click *Dial Plan* > *Extension List*.
2. Click *Add*.
3. In the *List Extension* field, type the number that you want to assign to the new extension list. Do not select a number that is currently in use by the system as either an extension or as the number of an extension list.

   You may use the default extension number.
4. Type an asterisk preceding the extension number. By convention, the asterisk indicates that the number represents an extension list.
5. In the *Name* field, type the name that you want to assign to the new extension list. Names can include uppercase and lowercase alphanumeric characters, spaces, underscores, and hyphens.
6. If you want calls to cycle through the extensions in the list, enable the Cycle Extensions check box. Each time the system accesses the extension list, it uses the next extension in the list. Calls effectively progress through the list to balance the load of calls. If you disable the Cycle Extensions check box, the extension selection always starts from the top of the list.

   If an extension in the list has a higher priority, the system uses the highest priority extension regardless of the Cycle Extension setting.
7. To add an extension to the list:
   a. If the list does not include any members, click the check boxes next the extension that you want to add to the list.
   b. If the list already has members, click *Show all* to display a list of extensions that you can add to the list's membership.

   NOTE*: You can toggle between the* Show all *and* Show members only *buttons to display extensions that have membership in the list and the extensions that are not members of the list but which you can add to the list, and to confirm your changes.*
8. To change the priority of an extension, enter a priority number in the field next to the selected extension (from a high of 1 through a low of 99).

   The default value is 50. When the system accesses an extension list, it first attempts to use the highest priority extension.
9. Click *Apply* to make the changes and keep this window open or click *OK* to make the changes and close the window. Click *Reset* to restore the

settings back to their original status or click *Cancel* to return to the previous window without putting the changes into effect.

Example: If the extension list contains extensions that you assigned to T1 channels, you can assign unique priorities to each extension. If you instruct the system to place an outgoing call using the T1 line, it attempts to use the highest priority extension/channel first, and, if the first is unavailable, tries the next highest priority extension/channel, and so on. Priorities range from 1 (highest) through 99 (lowest).

CAUTION: *If you add an extension list, change the dial plan configuration file to create a destination route to the new list. This enables the system to route calls to the new list.*

Modifying an Extension List

To modify an extension list:

1. Click *Dial Plan* > *Extension Lists*.
2. Click an extension list.
3. In the List Extension field, type an extension number for the extension list.
4. In the *Name* field, type a name for the extension list.

If you change the name of an extension list, you invalidate any aspect of the dial plan that refers to the name. You must change all references to the extension list name in the dial plan configuration file. If you use an editor to make changes (rather than modifying the dial plan from within the NBX NetSet utility), reimport the dial plan.

5. If you want calls to cycle through the extensions in the list, enable the Cycle Extensions check box. Each time the system accesses the extension list, it uses the next extension in the list. Calls effectively progress through the list to balance the load of calls. If you disable the Cycle Extensions check box, the extension selection always starts from the top of the list.

   If an extension in the list has a higher priority, the system uses the highest priority extension regardless of the Cycle Extension setting.

6. To add an extension to the list:
   - **a** If the list does not include any members, click the check boxes next the extension that you want to add to the list.
   - **b** If the list already has members, click *Show all* to display a list of extensions that you can add to the list's membership.

***NOTE**: You can toggle between the* Show all *and* Show members only *buttons to display extensions that have membership in the list and the extensions that are not members of the list but which you can add to the list, and to confirm your changes.*

7 To change the priority of an extension enter a priority number in the field next to the extension (from a high of 1 through a low of 99).

The default priority value is 50. When the system accesses an extension list, it attempts to use the highest priority extension first.

8 Click *Apply*, or *OK* to enable your changes and exit the dialog box.

Removing an Extension List

The system does not let you remove an extension list that the dial plan is using, even if that extension list is empty. You must remove the extension list from the dial plan before you can delete the extension list.

To remove an extension list:

1 Click *Dial Plan* > *Extension Lists*.

2 Select the extension, or extensions, that you want to delete and click *Remove Selected*. To select all extensions, enable the *Select* check box.

3 Click *OK* to confirm.

***CAUTION:** Do not remove any of the predefined lists (lists *0001* through *0008).*

Managing Dial Plan Tables

The system associates a normal dial plan table and a Least Cost Routing table with each device. Devices include telephones, Analog Line Card ports, or Digital Line Card ports. A telephone without an assigned table does not have permission to dial and is flagged in the dial plan report. For details, see "Generating a Dial Plan Report" on page 280.

Determining Which Devices Use Dial Plan Tables

You can view or change the devices associated with a particular dial plan:

1 Click *Dial Plan* > *Tables*.

2 From the Dial Plan Tables list:

- Select *(None)* to list devices that are not assigned to any table.

- Select a dial plan table for which you want to list associated devices, which displays:
  - **Dial Plan Table ID** — The identification number of the dial plan table as specified in the dial plan configuration file
  - **Dial Plan Table Name** — The name of the dial plan table

3 Click *Normal* to see which devices use table ID 1 (in this example) as the Normal table.

4 Click *Least Cost* to see which devices use table ID 1 as the Least Cost table. Each device can use only one normal and one least cost table.

5 To add a device to the *Devices Using Table* list, click *Show All* and then click to select an available device from the list.

6 To add a device:

a If the list does not include any devices, click the check boxes next to the device extensions that you want to add to the list.

b If the list already has devices, click *Show all* to display a list of devices that you can add to the list's membership.

***Note**: You can toggle between the **Show all** and **Show members only** buttons to display devices that have membership in the device list and the devices that are not members of the list but which you can add to the list, and to confirm your changes.*

7 Click *Apply* to make the changes and keep this window open, click *OK* to make the changes and close the window, or click *Cancel* to return to the previous window without putting the changes into effect.

Removing a Dial Plan Table

You must *not* remove any of the predefined tables (Internal, Incoming, or Least Cost).

***CAUTION:** You cannot remove a dial plan table if a device is using it. To remove the table, first remove all devices from the* Devices Using Table *list.*

To remove a dial plan table:

1 Click *Dial Plan > Tables*.

2 Select the table, or tables, that you want to delete and click *Remove Selected*. To select all tables, enable the *Select* check box.

3 Click *OK* to confirm.

Managing Dial Plan Pretranslators

Pretranslators are tables in the dial plan configuration file. Each entry in a pretranslator table contains a string of one or more digits that the system compares to incoming or outgoing digits. When the digits match an entry in the table, the system performs the associated pretranslator operations.

For more information, see:

- Identifying Devices Using Pretranslators
- Creating a Pretranslator for VTL Calls
- Identifying Devices Using Pretranslators for CLI
- Removing a Pretranslator from the Dial Plan

Identifying Devices Using Pretranslators

To view a list of devices and their associated pretranslators, or to associate a pretranslator with a specific device:

1. Click *Dial Plan* > *Pretranslators*.
2. Click a pretranslator or click *(None)* for devices that have no pretranslator.

   The system displays the *Device Using* window. If you selected *(None)*, you see a list of devices that do not use a pretranslator. Table 58 describes each field. The fields are the same for the *Devices Using Pretranlator for CLI* dialog box.
3. To add a device to the *Devices Using Pretranslator* list, click *Show All* and then click to select an available device from the list.
4. Click *Apply,* or *OK* to save your changes and exit from the window.

Table 58 Pretranslator Fields

Field	Purpose
Pretranslator ID	The identification number of the pretranslator as specified in the dial plan.
Pretranslator Name	The name of the pretranslator as specified in the dial plan.
Selected Devices (Members)	Devices currently using the pretranslator.
Unselected Devices (Nonmembers)	Devices not using the pretranslator.

To enable a specific pretranslator, update the dial plan. See "Importing and Exporting Dial Plan Configuration Files" on page 275.

Creating a Pretranslator for VTL Calls

Calls from one system to another system over a VTL connection include caller ID information that includes the IP address of the caller's system and the caller's extension. The "*" character separates each field of numbers in this caller ID string. For example, if extension 1002 on System A calls someone on system B over a VTL connection, the display panel on the System B telephone displays `10*234*208*2*1002`, which indicates an incoming call from extension 1002 on the system with the IP address 10.234.208.2.

If the System B dial plan has a pretranslator that removes the IP address when the call arrives at System B, (see Figure 14 on page 298), the display panel on the System B telephone displays the calling extension and no IP address or "*" characters. This solution works well when the extensions on System A and System B do not overlap, for example, System A user extensions are 1000-1999 and System B extensions are 2000-2999.

Call Detail Reports (CDR) Records

CDR records incorporate caller ID information to identify a caller. VTLs transmit a maximum of 30 characters for the caller ID. Because the caller ID for incoming VTL calls also includes the IP address before the extension number, the 31st and subsequent characters are dropped from the caller ID. Consequently, the CDR records might contain abbreviated caller ID information. If you enable CDR and VTL, add a pretranslator to avoid inaccurate data.

Site Codes

If the dial plan on System B uses a site code, such as 69, for VTL calls to System A, you can create a pretranslator that prepends the site code after it removes the IP address. (See Figure 15 on page 299.) This pretranslator would provide caller ID information that the System B extension can use to return a call to the System A extension. For example, a call from System A (10.234.208.2) extension 1002 would appear on a System B telephone's display panel as `691002` instead of `10*126*14*200*1002`. The pretranslator removes the IP address and prepends the calling extension with the System A site code, 69.

You might choose to not implement this pretranslator if calls from System A can hop off at System B onto a PRI line because the site code would be included as caller ID information about the PRI line, and that caller ID

information would be meaningless to someone outside the system. For hop-off calls, you can create a separate pretranslator.

VTL Calls, Caller ID and Hop Off

If a VTL call from System A to System B hops off System B and onto an ISDN PRI trunk, the "*" characters in the caller ID string can present problems for the PRI service. The PRI service cannot interpret the "*" symbols so it ignores the caller ID string it has received and instead uses the PRI line telephone number. For example, if you must dial 1-508-555-1234 to access the PRI externally, that number is used for the outgoing caller ID. If System A or System B has CLIR (Calling Line Identity Restriction) enabled, the PRI service ignores the CLIR setting and it sends the PRI line telephone number as the caller ID.

If you have a pretranslator on System B that removes the IP address from the caller ID string of incoming VTL calls, then the caller ID will be the extension of the telephone making the call. If system A and/or System B has CLIR enabled, then CLIR will be in effect. The only exception is for emergency calls (as defined in System B's dial plan), which never have caller ID blocked.

Figure 14 shows an example of a pretranslator that removes the "*" character from VTL calls that originate on a system with the IP address 10.234.208.2. The Value column of the PreTranslatorOperation Create line of Figure 14 specifies how many digits to strip from the beginning of the string. That value depends on the length of the received IP address. In the example, the IP address, 10*234*208*2, is 12 digits, and then you must also count the trailing "*" in the string. That trailing "*" is the character that separates the IP address from the caller extension and you must count it when you specify the number of digits to remove.

Figure 14 Pretranslator to Remove IP Address

```
PreTranslator Create 2 VTL
/                            PreTransId Entry Digits
/                            ---------- ----- ------
PreTranslatorEntry Create               2     1  10*234*208*2*

/                           PreTransId Entry OperId Operation  Value
/                           ---------- ----- ------ ---------  -----
PreTranslatorOperation Create           2     1       1 stripLead  13
```

Figure 15 shows an example of a pretranslator that removes the "*" character from VTL calls that originated on a system with the IP address 10.234.208.2 and prepends the site code, 69, of system 10.234.208.2.

Figure 15 Pretranslator to Remove IP Address and Prepend Site Code

```
PreTranslator Create 2 VTL
/                              PreTransId Entry Digits
/                              ---------- ----- ------
PreTranslatorEntry Create                2     1  10*234*208*2*

/                             PreTransId Entry OperId Operation  Value
/                             ---------- ----- ------ ---------  -----
PreTranslatorOperation Create           2     1       1 stripLead  13
PreTranslatorOperation Create           2     1       2 prepend    69
```

To add a pretranslator for VTL caller ID issues:

1. Open your dial plan for editing as described in "Accessing the Dial Plan" on page 274.
2. Search for the section titled Pretranslators.
3. Add a new pretranslator for each system from which you will be receiving calls over a VTL.
4. Save the edited dial plan and import it into the system. For more information, see "Importing and Exporting Dial Plan Configuration Files" on page 275.
5. Specify the devices that use the pretranslator. See "Adding VTL Devices to the Pretranslators (Optional)" on page 338.

Identifying Devices Using Pretranslators for CLI

To view a list of devices that use a particular pretranslator to present Calling Line ID (CLI) information about outgoing calls:

1. Click *Dial Plan* > *Pretranslators.*
2. Click a pretranslator or click *(None)* for devices that have no pretranslator.
3. Click the Device Using CLI tab

   If you selected *(None)*, you see a list of devices that do not use a pretranslator for Calling Line ID.
4. To add a device to the list, click *Show All* and then click to select an available device from the list. See Table 58 for field descriptions.

5 Click *Apply* to make the changes and keep this window open, click *OK* to make the changes and close the window, or click *Cancel* to return to the previous window without putting the changes into effect.

Removing a Pretranslator from the Dial Plan

To remove a pretranslator:

1 Click *Dial Plan* > *Pretranslators* and select a pretranslator from the scroll list.

2 Select the pretranslator, or pretranslators, that you want to delete and click *Remove Selected*. To select all pretranslators, enable the *Select* check box.

3 Click *OK*.

CAUTION: *You cannot remove a pretranslator if any device is currently using it. If you want to remove the pretranslator, first remove all devices from the* Devices Using *list.*

Configuring the Dial Plan for the 4ESS Protocol (T1)

The 4ESS protocol, used on T1 Digital Line Cards that are configured for PRI operation, requires specific configuration entries in the system dial plan. If you purchase the 4ESS protocol and SDN (Software Defined Network) service from your long-distance carrier, you must make dial plan changes similar to those outlined in "Configuring the Dial Plan for SDN Calls" on page 300. If you want to make long distance calls or international long distance calls using the 4ESS protocol, you must make dial plan changes similar to those outlined in "Configuring the Dial Plan for North American Long Distance" on page 301 and "Configuring the Dial Plan for International Long Distance" on page 301.

Configuring the Dial Plan for SDN Calls

If you use the 4ESS protocol and want to make SDN calls, in the system dial plan, configure a unique route to use for SDN calls and include the letters SDN at the beginning of the dial string.

Example: The dial plan entry shown in Figure 16 adds the characters SDN, which must be upper case letters, before the long-distance dialed digits. This example assumes that SDN calls use route 4.

Figure 16 Dial Plan Entries for SDN

```
/                                Route Entry OperID Operation Value
/                                ----- ----- ------ --------- -----
DestinationRouteOperation Create   4     1      1    prepend    SDN
```

Configuring the Dial Plan for North American Long Distance

If you use the 4ESS protocol and want to make long-distance calls, in the system dial plan, remove any digits that are dialed by telephone users to access the long-distance service from the dial string. For example, if telephone users normally dial 9 and then 1 to obtain a long-distance dial tone, and then dial a 10-digit number, the dial plan must remove the 9 and the 1 and present only the 10-digit number to the long-distance carrier. Otherwise, the 4ESS protocol rejects the call.

Example: If you use route 1 in the dial plan for Long Distance, and telephone users must dial 91 to make a long-distance call, the dial plan entries shown in Figure 17 remove the first two digits (91) and submit the remaining 10 digits to the long-distance carrier.

Figure 17 Dial Plan Entries for North American Long Distance

```
Table Create 1 Internal 4 Digit Extensions
/                ID Entry Digits Min Max  Class         Prio Route
/                -- ----- ------ --- ---  ------------ ---- -----
TableEntry Create  1     2 91      12  12  LongDistance    0     1

/                              Route Entry OperID Operation Value
/                              ----- ----- ------ --------- -----
DestinationRouteOperation Create   1     1      1    stripLead    2
```

Configuring the Dial Plan for International Long Distance

If you use the 4ESS protocol and you want to make international long-distance calls, in the dial plan, remove from the dial string the digits 9011 that are dialed by telephone users to access the international long-distance service. For example, if the telephone user dials the string 9-014-1234-567890, the dial plan must remove 9011 before it passed the dialed digits to the long-distance carrier or the 4ESS protocol rejects the call. See Figure 18.

Figure 18 Dial Plan Entries for International Long Distance

```
Table Create 1 Internal 4 Digit Extensions
/                ID Entry Digits Min Max  Class          Prio Route
/                -- ----- ------ --- ---  ------------   ---- -----
TableEntry Create  1     3 9011    12  64  International    0     1

/                              Route Entry OperID Operation Value
/                              ----- ----- ------ --------- -----
DestinationRouteOperation Create   3      2      1    stripLead    4
```

Dial Plan Configurations and VPIM

With Voice Profile for Internet Mail (VPIM), telephone users on one system can send voice mail to a user on another VPIM-compliant system. For detailed information about VPIM and how to configure VPIM settings, see "Voice Profile for Internet Mail" on page 223

To send a voice mail message to a user on another VPIM-compliant system, a telephone user first composes the voice mail message, using the commands in the user's voice mailbox. Depending on how you configure the system's dial plan, the telephone user can specify the destination in two ways:

- If the dial plan is configured for site codes, the telephone user specifies the destination site code followed by the extension of the person for whom the voice mail message is intended.
- If the dial plan is configured without site codes, the telephone user specifies the extension of the person for whom the message is intended. This requires that each site use a unique extension range for telephones.

A telephone user who knows the IP address of a VPIM-compliant voice mail system and the extension of a person who uses that system can compose a voice mail message and then send it using these steps:

1. Dial the IP address, pressing the * key after each field in the address, including the last field.
2. Dial the extension of the person followed by # key.

You must decide whether to use site codes or unique extension ranges when you configure the dial plan.

Configuring the Dial Plan for VPIM

To define a VPIM connection between two systems, create entries in the dial plan for the following items:

- The digit sequence that a telephone user must dial to access the VPIM connection
- The route number that is used to access the other NBX system
- The extension list to which the VPIM route belongs
- The operations that must be performed on the dialed digits to create the appropriate outgoing digit sequence

Figure 19 contains sample lines which, when added to an existing dial plan, implement VPIM connections to two other systems, one in Atlanta and one in Dallas. Table 59 explains each entry.

Figure 19 Dial Plan with VPIM Implementation Commands

```
Table Create 1 Internal Extensions
/                  Id Entry  Digits      Min Max Class            Prio Route
/                  -- -----  ----------- --- --- -------------    ---- -----
TableEntry Create   1    45  V82           5   5 WAN                 0   532
TableEntry Create   1    46  V83           6   6 WAN                 0   533


/                      Route Description
/                      ----- -----------
DestinationRoute Create   532 Atlanta VPIM Connection
DestinationRoute Create   533 Dallas VPIM Connection


/                           Route Entry DestinationExtension
/                           ----- ----- --------------------
DestinationRouteEntry Create   532     1 *0003
DestinationRouteEntry Create   533     1 *0003


/                              Route Entry OperId Operation  Value
/                              ----- ----- ------ ---------  -----
DestinationRouteOperation Create   532     1      1 stripLead  3
DestinationRouteOperation Create   532     1      2 prepend    10*234*101*222*
```

Table 59 Explanation of Entries in Figure 19

Field	Purpose
Table Create 1 Internal Extensions	
	This command is present in all default dial plans. It is included here as a reference point for subsequent commands.
TableEntry Create 1 45 V82 5 5 WAN 0 532	
TableEntry Create 1 45	This portion of the command creates entry 45 in dial plan table 1 (the *Internal Extensions* table). The choice of 45 as the entry number depends on how many entries exist in table 1. This example assumes that the highest number assigned to a previously existing entry was 44.
V82 (Digits column)	The required upper case letter V indicates that this is a VPIM connection. The number 82 indicates that telephone users must dial 82 to access the VPIM connection and then dial the extension they want to reach. You can select any number of digits for a site code. The selected number must not conflict with other dial plan entries. This example assumes that 82 is not used in any other way in the dial plan. **NOTE**: Long digit sequences can a create an opportunity for dialing errors.
Min (5) Max (5)	Indicates that the total digit sequence the telephone user dials is 5 digits. The first two digits are the site code (82 in this example) and the remaining 3 digits are the destination extension.
Class (WAN)	Indicates that this call is classified as *WAN*. All VPIM calls have this classification.
Priority (0)	This field is unused by the dial plan; the default value is zero (0).
Route (532)	In this example, the VPIM connection to the other NBX system uses route 532. The route number must be unique in the dial plan and in the range of 1–32768.
DestinationRoute Create 532 Atlanta VPIM Connection	
	This command creates route number 532 and names it *Atlanta VPIM Connection*.
DestinationRouteEntry Create 532 1 *0003	
	This command (mandatory for all VPIM routes) assigns route 532 to the extension list *0003.
DestinationRouteOperation Create 532 1 1 stripLead 3	

Table 59 Explanation of Entries in Figure 19 (continued)

Field	Purpose
	For DestinationRoute 532, entry 1, this command creates operation 1, which removes the first three digits, including the letter V, from the digit string, leaving only the extension that the telephone user dials.
DestinationRouteOperation Create 532 1 2 prepend 10*234*101*222*	
	For DestinationRoute 532, entry 1, this command creates operation 2, which places the string 10*234*101*222* in front of the extension. This string represents the IP address of the target NBX system. You must use the star character (*) to separate the fields within the IP address and to separate the IP address from the extension field.

Dial Plan Configuration File Commands

This section provides the syntax and description of each command used to create the information in the dial plan configuration file. See these sections for detailed information:

- "Dial Plan Command Format" on page 264.
- Table 60 on page 306, which categorizes and summarizes all the dial plan commands.
- "Dial Plan Command Summary" on page 305, which is a description of each component of dial plan commands.
- "List of Dial Plan Commands" on page 307, which is the alphabetical list of dial plan commands that provides a detailed description and syntax of each command.
- "Sample Solutions Using Dial Plan Configuration File Commands" on page 320 shows how these commands are implemented in a dial plan. You can also open and examine any of the dial plans that are shipped with your system.

Dial Plan Command Summary

Table 60 provides a brief summary of the dial plan commands. The summary lists and categorizes these commands in the order that they might logically appear in a working dial plan.

See "List of Dial Plan Commands" on page 307 for a complete list and description of each dial plan command, including syntax and arguments.

Command syntax is case insensitive. In the sample dial plans supplied with the system, and in this section, commands use upper and lower case to make them easier to read.

An entry that begins with "*n*" for example, *n*DialPlanID, indicates an integer field. Integer IDs are used in many places, and must be within the range 1 through 32768. The system reserves dial plan table ID numbers 1, 2, and 3 for Internal, Incoming, and Least Cost Routing, respectively.

An entry that begins with "*sz*" (for example, *sz*Description) indicates a field composed of alphanumeric characters. Acceptable characters are a through z, A through Z, and 0 through 9.

Each line in the configuration file must contain a complete command. The system reads all lines in the configuration file, and ignores only those lines containing one or more syntax errors. The system treats any line that begins with / (forward slash) as a comment and ignores it.

CAUTION: *Do not place comments at the end of a command line.*

Table 60 Dial Plan Command Summary

Command Name	Description
Table Create	Creates a dial plan table.
TableEntry Create	Creates an entry in a dial plan table.
DestinationRoute Create	Creates a route that specifies the primary and alternative destination device of a call.
DestinationRouteEntry Create	Creates a destination route entry that identifies a single destination device or device list.
DestinationRouteOperation Create	Creates a digit manipulation operation for a destination route entry.
TimedRoute Create	Creates a timed route (a route that the system uses based on defined criteria for time of day and day of week).
TimedRouteEntry Create	Creates a timed route entry specifying either a time of day or system mode, day of the week criteria, and the destination route to use if that criteria are met.
TimedRouteOperation Create	Creates a digit manipulation operation for a timed route entry.

Table 60 Dial Plan Command Summary (continued)

Command Name	Description
PreTranslator Create	Creates a pretranslator entry and specifies a string of digits that are compared to the incoming digits.
PreTranslatorEntry Create	Creates a pretranslator entry and specifies a string of digits that are compared to the incoming digits.
PreTranslatorEntry Delete	Deletes a pretranslator entry or deletes all entries for a particular pretranslator.
PreTranslatorOperation Create	Creates a digit manipulation operation for a pretranslator entry.
ExtensionLength	Specifies the length of extension numbers for system devices.
ExtensionRange	Specifies a range of extensions for each type of device.
ExternalSettings	Specifies settings for several aspects of external devices.

List of Dial Plan Commands

The dial plan commands are described in this section. They are listed in alphabetical order:

- DestinationRoute Create
- DestinationRouteEntry Create
- DestinationRouteOperation Create
- ExtensionLength
- ExtensionRange
- ExternalSettings
- PreTranslator Create
- PreTranslatorEntry Create
- PreTranslatorEntry Delete
- PreTranslatorOperation Create
- Table Create
- TableEntry Create
- TimedRoute Create
- TimedRouteEntry Create

- TimedRouteOperation Create

DestinationRoute Create

Syntax

```
DestinationRoute Create nRouteId szDescription
```

Description Creates a route that specifies the primary and alternative destination device of a call (for example, which CO Line or Digital Line Card port over which to route the call). If the destination route already exists, this command removes all of its entries and operations, and overwrites its description with the new information.

Arguments

nRouteId — An integer in the range 1 – 32768, uniquely identifying this destination route.

szDescription — The description or name of the destination route.

Example: This example creates destination route 3 and names it "Voice Application": `DestinationRoute Create 3 Voice Application`

DestinationRouteEntry Create

Syntax

```
DestinationRouteEntry Create nRouteId nEntryId szExtension
```

Description creates a destination route entry that identifies a single destination device or device list.

If the specified destination route entry already exists, this command overwrites it with the new information. During routing, the system checks the list of destinations in ascending *nEntryId* order (*nEntryId* 1 first).

Arguments

nRouteId — An integer in the range 1 through 32768.

nEntryId — An integer in the range 1 through 32768. The system checks the list of destinations in ascending *nEntryId* order, and uses the first available one.

szExtension — The extension of the destination device or device list. Note that the system does not dial this extension (that is, it neither checks the extension against a dial plan nor subjects it to Class of Service restrictions, digit manipulation, or routing) but instead uses the extension only to look up the device in the internal device directory.

Example: This example command creates, in route table 3, entry 1 and defines extension list *0003 as the destination for this route entry. Extension list *0003 contains the voice mail extensions/ports.

```
DestinationRouteEntry Create 3 1 *0003
```

DestinationRouteOperation Create

Syntax

```
DestinationRouteOperation Create nRouteId nEntryId nOperId
szOperation szValue
```

Description Creates a digit manipulation operation for a destination route entry. If the specified digit manipulation operation already exists, this command overwrites it with the new information. During routing the system processes the entire list of operations in ascending nOperId order (nOperId 1 first).

Arguments

RouteId — An integer in the range 1 through 32768.

nEntryId — An integer in the range 1 through 32768 specifying the destination route entry to which this operation applies.

nOperId — An integer in the range 1 through 32768. The system processes the list of operations in ascending nOperId order.

szOperation — The name of the digit manipulation operation to perform: stripLead, stripTrail, replace, prepend, append.

szValue — A value used by the operation, either the string of digits to prepend, append, replace with, or the number of digits to strip.

Example: This example command creates, for destination route 3, entry 1, an operation numbered 1, with the associated function stripLead, and an argument of 1, indicating that the command removes (strips) one leading digit from the dialed number before dialing.

```
DestinationRouteOperation Create 3 1 1 stripLead 1
```

ExtensionLength

Syntax

```
ExtensionLength nExtensionLength
```

Description The length of extension numbers for system devices. The default is 4 for V3000, V3001R, and V5000 systems. The default is 3 for NBX 100 systems.

Arguments

nExtensionLength — specifies either 3 to designate a a 3-digit dial plan, or 4 to designate a 4-digit dial plan.

ExtensionRange

Syntax

ExtensionRange szExtensionType szLowestExtension szHighestExtension

Description A range of extensions for each type of device. When the system automatically generates extensions it assigns them from within this range. When you manually generate an extension number, verify that it is within the valid range. During a dial plan import operation, the system does not validate that existing extensions are within the specified range. 3Com *strongly* recommends that you configure the dial plan *before* you define any devices in the system.

Arguments

szExtensionType — One of these: Telephone, Park, Auto Attendant, Hunt Group, External.

szLowestExtension — The lowest desired extension for this device type.

szHighestExtension — The highest desired extension for this device type.

Example: These commands define the extension range for telephones as 100 through 449, for call park as 601 through 609, for Auto Attendants as 500 through 599, for hunt groups as 450 through 499, and for external lines as 600 through 799.

```
ExtensionRange Telephone 100 449
ExtensionRange Park 601 609
ExtensionRange Autoattendant 500 599
ExtensionRange HuntGroup 450 499
ExtensionRange External 600 799
```

CAUTION: *Do not define extension ranges that overlap. The only exception is* Park*, which must be within the* External *range.*

ExternalSettings

Syntax

```
ExternalSettings szExternalKeysetPrefix
szFirstAutoDiscoverExtension szDefaultAutoExtension
```

Description Specifies settings for several aspects of external devices.

Arguments

szExternalKeysetPrefix — The digits that are prepended to external calls made in Keyset mode. This is used to determine the Class of Service (CoS) for external calls made in Keyset mode. Typical values for this digit are 8, 9, or 0 (zero). This prefix is set to the appropriate number in each country's dial plan.

Example: In the default internal dial plan table, the digit 9 instructs the system to connect the call to an external line. When a telephone has a button mapped to an external device, and the user places a call using that external device, the system prepends the *szExternalKeysetPrefix* digit to the digits dialed by a user; then the system applies the dial plan tables to determine call Class of Service.

szFirstAutoDiscoverExtension — The first extension used when autodiscovering external devices. This must be in the specified range of lowest/highest external extensions.

The system assigns extensions starting with this number and incrementing upward. For information about the Auto Discovery topic, see "Using Auto Discovery for Initial System Configuration" in the *NBX Installation Guid*e.

The default value for a 3-digit system is 750, and for a 4-digit system is 7250. Typically, systems do not use all of the extensions from 600 through 799 (or 6000 through 7999). If, however, the system uses all of these extensions and needs another one, it starts looking from the beginning of the range and selects the first unused one.

szDefaultAutoExtension — The default extension the system uses for forwarding incoming calls. This is always 500.

The system must direct each incoming call (on an external line) to an extension. After you import the dial plan configuration file, and complete the Auto Discovery process, you can manually configure the extension for each analog line and each Digital Line Card channel, if you want.

PreTranslator Create

Syntax

```
PreTranslator Create nPreTranslatorId szDescription
```

Description Creates a pretranslator. If the pretranslator already exists, this command removes all of its entries and operations, and overwrites its description with the new information.

Arguments

nPreTranslatorId — An integer in the range 1 through 32768.

szDescription — The description or name of the pretranslator.

Example: This command creates a pretranslator, designates it as the first one (number 1) and give it the title "4-to-3-digit DID/DDI pretranslator."

```
PreTranslator Create 1 4-to-3-digit DID/DDI pretranslator
```

PreTranslatorEntry Create

Syntax

```
PreTranslatorEntry Create nPreTranslatorId nEntryId szDigits
```

Description Creates a pretranslator entry and specifies a string of digits that are compared to the incoming digits. If the pretranslator entry already exists, this command overwrites it with the new information.

Arguments

nPreTranslatorId — An integer in the range 1 through 32768.

nEntryId — An integer in the range 1 through 32768.

szDigits — The digits to compare to the incoming digits.

Example: These example commands create, in pretranslator 1, entries 1 through 10, each of which looks for a different single digit (0 through 9) in the incoming digits.

```
PreTranslatorEntry Create 1 1 0
PreTranslatorEntry Create 1 2 1
PreTranslatorEntry Create 1 3 2
PreTranslatorEntry Create 1 4 3
PreTranslatorEntry Create 1 5 4
PreTranslatorEntry Create 1 6 5
PreTranslatorEntry Create 1 7 6
PreTranslatorEntry Create 1 8 7
PreTranslatorEntry Create 1 9 8
PreTranslatorEntry Create 1 10 9
```

PreTranslatorEntry Delete

Syntax

```
PreTranslatorEntry Delete nPreTranslatorId nEntryId
```

Description Deletes a pretranslator entry or deletes all entries for a particular pretranslator.

Use caution when using this command to delete Pretranslator entries in an existing dial plan. In general, it is best to delete all tables, routes, and pretranslators at the beginning of each dial plan configuration file. This precaution avoids the potential conflicts or unpredictable actions caused by importing new dial plan entries on top of an existing dial plan.

For instructions on how to edit the dial plan configuration file to delete existing tables, routes, and pretranslators, see *"Creating Dial Plan Configuration Files" on page 274*.

Arguments

nPreTranslatorId — An integer in the range 1–32768.

nEntryId — An integer in the range 1–32768 or * for all entries.

Example: This command deletes pretranslator entry 3 from pretranslator 2.

```
PreTranslatorEntry Delete 2 3
```

This command deletes all pretranslator entries from pretranslator 2.

```
PreTranslatorEntry Delete 2 *
```

Normally this command is not necessary. It is better to delete an entire dial plan rather than import a new dial plan over it. To accomplish this, 3Com recommends using specific commands at the top of every dial plan configuration file. For an example of this technique, see "Creating Dial Plan Configuration Files" on page 274.

PreTranslatorOperation Create

Syntax

```
PreTranslatorOperation Create nPreTranslatorId nEntryId
nOperId szOperation szValue
```

Description Creates a digit manipulation operation for a pretranslator entry. If the specified digit manipulation operation already exists, this command overwrites it with the new information. During pretranslation, the system processes the list of operations in ascending *nOperId* order (*nOperId* 1 first).

Arguments

nPreTranslatorId — An integer in the range 1 through 32768.

nEntryId — An integer in the range 1 through 32768 specifying the pretranslator entry to which this operation applies.

nOperId — An integer in the range 1 through 32768. The system processes the list of operations in ascending nOperId order (*nOperId* 1 first).

szOperation — The name of the digit manipulation operation to perform. Values are: stripLead, stripTrail, replace, prepend, append.

szValue — The value to use in the operation, either the string of digits to prepend, append, replace with, or the number of digits to strip.

Table Create

Syntax

```
Table Create nDialPlanTableId szDescription
```

Description Creates a dial plan table to control the routing of calls placed by devices. Dial plan tables apply to internal devices such as telephones, incoming calls from outside the system, and Least Cost Routes. If the dial plan table already exists, this command removes all entries from the table, and fills the table with the new information.

Arguments

nDialPlanTableId — An integer in the range 1 through 32768. The default dial plan tables use ID numbers 1 through 3:

1 — Internal dial plan table

2 — Incoming dial plan table

3 — Least Cost Routing table

szDescription — The description or name of the dial plan table. the NBX NetSet utility uses this name to refer to the table.

Example: This example command creates dial plan table 1 and names it "Internal 4 Digit Extensions."

```
Table Create 1  Internal 4 Digit Extensions
```

TableEntry Create

Syntax

```
TableEntry Create nDialPlanTableId nEntryId szDigits
nMinDigits nMaxDigits szCallClass nPriority nRouteId
```

Description Creates an entry in a dial plan table that specifies a string of digits that are compared to the dialed digits. If the dial plan table entry already exists, this command overwrites it with the new information.

Dial plan table entries make Class of Service and call routing decisions based on the correspondence of dialed digits and table entry digits.

Arguments

nDialPlanTableId — An integer in the range 1 through 32768. The system reserves three ID numbers:

1 — Internal dial plan table

2 — Incoming dial plan table

3 — Least Cost Routing table

nEntryId — An integer in the range 1 through 32768. Each entry must have a unique ID. If two entries have the same ID, the system uses the entry closer to the bottom of the configuration file (the one processed last).

szDigits — A string of dialed digits in a dial plan entry.

nMinDigits — An integer specifying the minimum number of digits to collect.

nMaxDigits — An integer specifying the maximum number of digits to collect.

szCallClass — The call class for this dial plan entry. The call class corresponds to permissions granted to users in their Class of Service. Values are Internal, Local, LongDistance, International, WAN, TollFree, Emergency, COCode, Wireless, Other, Toll, AlternateLong, Operator, TrunkToTrunk, Diagnostics, and NotAllowed.

nPriority — Not presently used. Always set to zero (0).

nRouteId — An integer specifying the ID of the route to use when this dial plan entry is matched. A route ID of zero (0) indicates that this entry has no defined route; digits are transmitted ed as soon as they are dialed.

Example: This example command creates (in table ID 1) table entry 1, which looks for 3 as the first digit in a 4-digit string (minimum and maximum number of characters are both specified as 4), classifies the call type as "Internal", assigns the call a priority of zero (the only acceptable priority in this product release). Because the destination is an internal extension, there is no need for a defined route so the route number is zero.

```
TableEntry Create  1  1  3  4  4  Internal  0  0
```

TimedRoute Create

Syntax

```
TimedRoute Create nRouteId nDefaultDestinationRouteId
szDescription
```

Description Creates a timed route (a route that the system uses based on defined criteria for time of day and day of week). If the timed route already exists, this command removes all of its entries and overwrites its description and *defaultDestinationRoute* with the new information.

Arguments

nRouteId — An integer in the range 1 through 32768 which uniquely identifies this timed route.

nDefaultDestinationRouteId — An integer in the range 1 through 32768 identifying the destination route the system must use if none of the entries in this timed route match the current time of day.

szDescription — A description or name of the timed route.

Example: This example command creates timed route 7 which uses destination route 1, defined in the "Routes" section of the system configuration file. The description of route 7 is "Business Hours Long Distance."

```
TimedRoute Create 7 1 Business Hours Long Distance
```

TimedRouteEntry Create

Syntax

```
TimedRouteEntry Create nRouteId nEntryId szStartTime
szEndTime szDaysOfWeek nDestinationRouteId
```

Description Creates a timed route entry specifying either a time of day or system mode, day of the week criteria, and the destination route to use if that criteria are met. If the specified timed route entry already exists, this command overwrites it with the new information. During routing, the system checks the list of timed route entries in ascending nEntryId order (*nEntryId* 1 first). The system performs any digit manipulation operations that apply to the specified destination.

Arguments

nRouteId — An integer in the range 1 through 32768.

nEntryId — An integer in the range 1 through 32768. The system checks the list of timed routes in ascending order based on nEntryId.

szStartTime — Start time in 24-hour format, for example, 13:30 for 1:30 p.m. You can use either 24:00 or 00:00 to specify midnight. Instead of specifying times, you can enter a system mode name (*open, closed, lunch*, or *other*). For each system mode, the system knows the start and stop times. If you use one of the system modes, both szStartTime and szEndTime parameter must be the same.

You define start and end times for system modes through the NBX NetSet utility. Click System-Wide Settings > Business Hours*. Enter the times that you want and click* OK*.*

Example: If you define business hours from 8:00 to 17:00 on Mondays, Wednesdays and Fridays, and from 9:00 to 18:00 Tuesdays and Thursdays, then a timed route entry both szStartTime and szEndTime set to "open" applies differently on Monday, Wednesday, and Friday than on Tuesday and Thursday.

You set the beginning and ending times for open, lunch, and other using the NBX NetSet utility. Click System-Wide Settings > Business Hours*. The system treats all times not included these three categories as closed.*

szEndTime — End time in 24-hour format, for example, "18:30" for 6:30 p.m. You can use either 00:000 or 24:00 to indicate midnight. If you use a system mode (open, lunch, or other) for szStartTime, you must use the same system mode for szEndTime.

szDaysOfWeek — A seven character mask in which each character position represents one day of the week, beginning with Sunday as the first character and ending with Saturday as the last character. The system excludes any day if a dot "." character appears in that day's position. (As a convention, you place the first letter of each day in the appropriate character position to indicate that the day is included, but you can use any letter you want; the presence of a dot "." in a given position excludes the day of the week and the presence of any other character in that position selects that day.

You use the *szDaysOfWeek* parameter to specify when this timed route is active. You can specify that the timed route entry apply to all days of the week. If you specify the start and end times for open mode differently on some days of the week than for other days, one timed route entry can operate differently depending on the day.

Example: The system interprets "SMT.T.S" (or "XXX.X.X") as "all days except Wednesday and Friday." The "dot" characters in positions four and six exclude the fourth and sixth days of the week (Wednesday and Friday).

nDestinationRouteId — The Id of the destination route to use if this entry's time of day and day of week criteria are met.

Example: This example command creates two entries, one to define the route to use during business hours (open) and the other to define the route when the business is closed.

The first entry is timed route 7, timed route entry 1. The two occurrences of the word "Open" instruct the system to use the start time and end time defined by the "open for business" hours, and the letters "SMTWTFS" indicate that this entry applies to all seven days of the week (Sunday through Saturday).

The number 6 designates destination route 6, defined in the system routes table. Because this entry applies to the "open for business" hours, route 6 could define a least cost route for outgoing long distance calls.

The second entry is timed route 7, timed route entry 2. The two occurrences of the word "Closed" instruct the system to use the start time and end time defined by the "business closed" hours, and the letters "SMTWTFS" indicate that this entry applies to all seven days of the week (Sunday through Saturday). The number 3 designates destination route 3, defined in the system routes table. Because this route applies to the "business closed" hours, route 3 could connect the incoming call to an Auto Attendant menu that tells the caller that the company is closed and gives instructions on how to leave a message and how to reach someone in an emergency.

```
TimedRouteEntry Create 7 1 Open Open SMTWTFS 6
TimedRouteEntry Create 7 2 Closed Closed SMTWTFS 3
```

TimedRouteOperation Create

Syntax

```
TimedRouteOperation Create nRouteId nEntryId nOperId
szOperation szValue
```

Description Creates a digit manipulation operation for a timed route entry. If the specified digit manipulation operation already exists, this command overwrites it with the new information. During routing, the system processes the list of operations in ascending *nOperId* order (*nOperId* 1 first).

CAUTION: *Timed route operations are performed* before *Destination Route operations. So if you strip a leading 9 using a TimedRouteOperation Create command verify that you don't mistakenly perform the same action in a DestinationRouteOperation Create command. If you made that error, you would lose the first dialed digit.*

Arguments

nRouteId — An integer in the range 1 through 32768.

nEntryId — An integer in the range 1 through 32768 specifying the timed route entry to which this operation applies.

nOperId — An integer in the range 1 through 32768. The system processes the list of operations in ascending *nOperId* order (nOperId 1 first).

szOperation — The name of the digit manipulation operation to perform: stripLead, stripTrail, replace, prepend, append.

szValue — The value used by the operation, either the string of digits to prepend, append, replace with, or the number of digits to strip.

Sample Solutions Using Dial Plan Configuration File Commands

This section describes several requirements that a customer might have, and for each one, provides a sample solution. An explanation follows each step in the solution.

For a detailed explanation of each command, see "Dial Plan Configuration File Commands" on page 305.

Customer Requirement 1. Assume that the telephone company passes 4-digit numbers to the system for each incoming telephone call (for example, numbers in the range 5200 through 5300). If the system uses 3-digit extensions in the range 200 through 300, you could define a single pretranslation operation that performed a *stripLead* to remove the first digit. For example, the system could remove the number five from an incoming number such as 5278, and pass the call to extension 278.

To accomplish the pretranslation:

```
PreTranslator Create 1 4-to-3-digit T1 DID/DDI Pretranslator
```

Explanation: Create pretranslator table 1, called "4-to-3-digit T1 DID/DDI Pretranslator."

```
PreTranslatorEntry Create 1 1 5
```

Explanation: Create, in pretranslator table 1, entry number 1, which applies when the first digit in the sequence is 5.

```
PreTranslatorOperation Create 1 1 1 stripLead 1
```

Explanation: For pretranslator table 1, PreTranslatorEntry 1, create the first PreTranslatorOperation. This performs a stripLead operation, removing a single leading digit from the incoming number.

Customer Requirement 2. Assume that the telephone company passes 10-digit numbers to the system for each incoming telephone call (for example, numbers in the range 4567-89-3000 through 4567-89-3500). If the system uses 4-digit extensions in the range 2000 through 2500, you can pass an incoming 10-digit number such as 4567-89-3210 to extension 2210 by using two pretranslation operations. The first operation performs a *stripLead* operation to remove the first 7 digits, leaving 210. The second would perform a *prepend* to add the digit 2 to the front of the number, creating 2210, which matches an extension within the extension range.

These entries in a dial plan configuration file would accomplish the pretranslation:

```
PreTranslator Create 1 10-to-3-digit T1 DID/DDI Pretranslator
```

Explanation: Create pretranslator table 1, called "10-to-3-digit T1 DID/DDI Pretranslator."

```
PreTranslatorEntry Create 1 1 4567893
```

Explanation: Creates the first entry in pretranslator table 1. This entry looks for sequence of digits 4567893.

This example assumes that all numbers begin with the same 7 digits (4567-89-3) and differ only in the last 3 digits. If this assumption is incorrect, you can add PreTranslatorEntry Create *lines to describe all of the possible variations.*

```
PreTranslatorOperation Create 1 1 1 stripLead 7
PreTranslatorOperation Create 1 1 2 prepend 2
```

Explanation: For PreTranslator table 1, PreTranslatorEntry 1, create the first PreTranslatorOperation. This performs a stripLead operation, removing the first seven leading digits from the incoming number.

Then create operation 2, which prepends the digit 2 to the remaining 3-digit number. The resulting 4-digit number matches one of the internal extensions in the system.

Customer Requirement 3. Assume that the telephone company assigns a group of 4-digit DID/DDI numbers from 6000 through 6199; however, you want to use internal telephone extensions from 3000

through 3199. Also, you want the number 6111 to connect the caller to an Auto Attendant line for the customer service group.

Add these lines to the dial plan configuration file:

```
PreTranslator Create 1 6XXX to 3XXX Translator
```

Explanation: Creates PreTranslator 1, and names it "6XXX to 3XXX Translator"

```
PreTranslatorEntry Create 1 1 6111
```

Explanation: Creates the first entry in Pretranslator 1. This entry looks for the specific sequence of digits 6111.

```
PreTranslatorOperation Create 1 1 1 replace 5502
```

Explanation: Creates the first operation associated with PreTranslator 1, PreTranslatorEntry 1. Defines a replace operation that replaces all digits in the incoming sequence (6111) with 5502. In this example, 5502 connects you to the Auto Attendant menu for customer service.

```
PreTranslatorEntry Create 1 2 6
```

Explanation: Creates, the second entry in Pretranslator 1; this entry looks for any incoming digit string beginning with the number 6.

```
PreTranslatorOperation Create 1 2 1 stripLead 1
```

Explanation: Creates the first operation associated with PreTranslator 1, PreTranslatorEntry 2. Defines a stripLead operation that removes (strips) the first (leading) digit from the incoming 4-digit sequence. This removes the 6 from the incoming numbers (6000 through 6199) leaving 3-digit numbers from 000 through 199.

```
PreTranslatorOperation Create 1 1 2 prepend 3
```

Explanation: Creates the second operation associated with PreTranslator 1, PreTranslatorEntry 2. Defines a prepend operation that adds the digit 3 at the beginning of the 3-digit string (created by the previous operation). The incoming numbers from 000 through 199 become numbers from 3000 through 3199.

The Incoming dial plan table might already contain this line. If necessary, modify the line to match.

```
TableEntry Create 2 4 3 4 4 Internal 0 0
```

Explanation: In table ID 2 (Incoming dial plan table) entry 4 instructs the system to look for 3 as the first in a sequence of 4 digits (both Min and Max are 4). If the system finds such a sequence, it assigns *Internal* as the

call class. The system does not use the number in the priority column, so it remains 0 (zero). The system directs the call to route 0 (zero), the default route for internal extensions.

Customer Requirement 4. Assume that the company is located in New York, and has two long distance telephone carriers: ABC, which provides a low-cost service to four Boston area codes (508, 617, 781, and 978), and DEF, which provides service to the rest of the United States. You want to use one 4-port Analog Line Card, connected to analog trunk lines owned by ABC, for all calls to the Boston area. You want to use the T1 line, which you lease from DEF, for all other long distance calls within the United States.

The system users dial 9 to get an outside line, 1 to obtain a long distance carrier, 3 digits to specify the area code, and 7 digits to specify the telephone number. To ensure that long distance calls are managed in the least-cost way that you want, you place these entries in the Internal dial plan table. The numbering of the entries assumes that the table has 46 entries before you make any additions. Columns in each table entry are titled: Command, Table Number, Entry Number, Digits, Min, Max, Class, Priority, and Route Number.

Add these lines to the dial plan configuration file:

```
TableEntry Create 1 47 91 12 12 LongDistance 0 2
```

Explanation: Creates, in table ID 1 (the Internal table), entry 47, which directs the system to look for the digits 91 at the beginning of any 12-digit sequence (Min and Max are both 12). If the system detects such a sequence, it assigns LongDistance as the class of service.

Because the system software does not use the priority value, the system leaves 0 (zero) as the value, and assigns the call to route 2 (the T1 route).

Dial plan entries are searched in sequential order. As soon as dialed digits match a dial plan entry, the dial plan acts on that match without further analysis. So if a previous dial plan entry (entries 1 through 46 in this example) was matched, entry 47 would not be found or used.

```
TableEntry Create 1 48 91508 12 12 LongDistance 0 1
```

Explanation: In table ID 1 (the Internal table), creates entry 48, which directs the system to look for the digits 91508 at the beginning of any 12-digit sequence (Min and Max are both 12). If the system detects such a sequence, it assigns LongDistance as the class of service. Because the system

software does not use the priority value, the system leaves 0 (zero) as the value, and assigns the call to route 1 (the route that uses the 4-port card).

```
TableEntry Create 1 49 91617 12 12 LongDistance 0 1
```

Explanation: In table ID 1 (the Internal table), creates entry 49, which directs the system to look for the digits 91617 at the beginning of any 12-digit sequence (Min and Max are both 12). If the system detects such a sequence, it assigns LongDistance as the class of service. Because the system software does not use the priority value, the system leaves 0 (zero) as the value, and assigns the call to route 1 (the route that uses the 4-port card).

```
TableEntry Create 1 50 91781 12 12 LongDistance 0 1
```

Explanation: In table ID 1 (the Internal table), creates entry 50, which directs the system to look for the digits 91781 at the beginning of any 12-digit sequence (Min and Max are both 12). If the system detects such a sequence, it assigns LongDistance as the class of service. Because the system software does not use the priority value, the system leaves 0 (zero) as the value, and assigns the call to route 1 (the route that uses the 4-port card).

```
TableEntry Create 1 51 91978 7 7 LongDistance 0 1
```

Explanation: In table ID 1 (the Internal table), creates entry 51, which directs the system to look for the digits 91978 at the beginning of any 12-digit sequence (Min and Max are both 12). If the system detects such a sequence, it assigns LongDistance as the class of service. Because the system software does not use the priority value, the system leaves 0 (zero) as the value, and assigns the call to route 1 (the route that uses the 4-port card).

In combination, the five lines in the internal table work with these two lines in the Routes section of the dial plan.

```
DestinationRoute Create 1 Boston Low-cost Carrier
DestinationRoute Create 2 T1 Line to DEF Telephone Company
```

Explanation: Creates two routes, numbered 1 and 2, with the names "Boston Low-cost Carrier" and "T1 Line to DEF Telephone Company."

```
DestinationRouteEntry Create 1 1 *0001
DestinationRouteEntry Create 2 1 *0001
```

Explanation: In route 1, creates entry number 1, which defines extension list *0001 (TLIM extensions) as the destination. Then creates, in route 2, an entry that defines extension list *0002 (Digital Line Card extensions) as the destination.

```
DestinationRouteOperation Create 1 1 1 stripLead 1
DestinationRouteOperation Create 2 1 1 stripLead 1
```

Explanation: Creates, in route 1, entry 1, operation number 1. This is a stripLead operation, which removes the first digit from the dialed string, then and passes the remaining digits to the carrier.

Customer Requirement 5. Assume that you want to transmit CLIP information about outgoing calls. You use internal telephone extension numbers from 3000 to 3099. There is no DDI/DID, so the T1 or E1 line has only a single number (555-555-1212). All incoming calls are routed by default to the Auto Attendant.

Add these lines to the dial plan configuration file:

```
PreTranslator Create 1 CLIP Internal Ext to Single Number
```

Explanation: Create pretranslator table 1 called "CLIP Internal Ext to Single Number."

```
PreTranslatorEntry Create 1 1 3
```

Explanation: For pretranslator 1, create entry 1, which applies when the first digit in the sequence is 3. (All internal telephone extensions begin with the number 3.)

```
PreTranslatorOperation Create 1 1 1 replace 555 555 1212
```

Explanation: For pretranslator 1, entry 1, create operation 1, which replaces the extension number with the string 555 555 1212.

Customer Requirement 6. Assume that you want to use two different long distance carriers at different times of the day, to obtain a cost saving. To select one long distance carrier from 7:30 a.m.) to 3:00 p.m., prepend 1010321 to each call. To select another carrier and obtain a lower rate from 3:00 p.m. until opening business hours the next day, prepend 1010220. This assumes the business is not open on weekends.

Add these lines to the dial plan configuration file:

```
TableEntry Create 1 99 91 12 12 LongDistance 0 27
```

Explanation: In Table 1 (Internal table) entry 99, creates an entry which looks for the digits 91 at the beginning of any 12-digit sequence (since both Min and Max are set to 12). If the system detects such a sequence, it assigns LongDistance as the class of service.

Because system software does not use the priority value, the system leaves 0 (zero) as the value, and assigns the call to route 27.

If Table 1 already contains an entry with 91 in the digits column, delete it and substitute the above TableEntry Create line.

```
TimedRoute Create 27 28 3PM Switchover
```

Explanation: Create TimedRoute 27, with a default DestinationRoute of 28. Assign the title "3PM Switchover" to TimedRoute 27.

```
TimedRouteEntry Create 27 1 7:30 15:00 .MTWTF. 29
```

Explanation: For TimedRoute 27, create entry 1, which applies from 7:30 a.m. through 3:00 p.m. Monday through Friday. The route to use is 29.

```
DestinationRouteCreate 29 Open Hours Carrier
```

Explanation: Create DestinationRoute 29, and call it "Open Hours Carrier."

```
DestinationRouteEntry Create 29 1 *0002
```

Explanation: For DestinationRoute 29, create entry 1, which uses extension list *0002, the extension list that contains all extensions associated with Digital Line Cards.

```
DestinationRouteOperation Create 29 1 1 stripLead 2
```

Explanation: For DestinationRoute 29, entry 1, create operation 1, which strips 2 digits (9 and 1) from the beginning of the dialed string.

```
DestinationRouteOperation Create 29 1 2 prepend 1010321
```

Explanation: For DestinationRoute 29, entry 1, create operation 2, which prepends 1010321 to select the long distance carrier to use from 7:30 a.m. Monday through Friday.

```
DestinationRoute Create 28 Carrier After 3pm and Closed
```

Explanation: Create DestinationRoute 28 and call it "Carrier After 3 p.m. and Closed."

```
DestinationRouteEntry Create 28 1 *0002
```

Explanation: For DestinationRoute 28, create entry 1, which uses extension list *0002, the extension list that contains all extensions associated with Digital Line Cards.

```
DestinationRouteOperation Create 28 1 1 stripLead 2
```

Explanation: For DestinationRoute 28, entry 1, create operation 1, which strips 2 digits (9 and 1) from the beginning of the dialed string.

```
DestinationRouteOperation Create 28 1 2 prepend 1010220
```

Explanation: For DestinationRoute 28, entry 1, create operation 2, which prepends 1010220 to select the other long distance carrier.

Route 28 is the default route, so it is used at all other times than those defined for route 29.

Example 1 If you make a long distance call at 2:00 p.m. on any Tuesday, the system uses these timed route definitions, and:

- Determines that the date is a valid business date.
- Determines that the time is prior to 3:00 p.m.
- Selects timed route 29.
- Prepends 1010321 to the outgoing call to select the first long distance carrier.

Example 2 If you make a long distance call at any time on any Saturday, the system uses these timed route definitions, and:

- Determines that the date is not a valid business date.
- Selects timed route 28.
- Prepends 1010220 to the outgoing call to select the second long distance carrier.

12 VIRTUAL CONNECTIONS

This chapter describes these elements of the system:

- Overview of Virtual Tie Lines
- TAPI Route Points
- TAPI Settings

For more information about these topics and configuration procedures, see the online Help.

Overview of Virtual Tie Lines

A Virtual Tie Line (VTL) provides a way to make calls between system sites that are separated geographically but tied together by a Wide Area Network (WAN). VTLs are a licensed feature of the systems. V3000, V3001R, and V5000 systems can support up to 48 simultaneous VTL connections. NBX 100 systems can support up to 8 simultaneous VTL connections

On any system, you can use a VTL connection either for an incoming VTL call from any site or for an outgoing VTL call to any site. A VTL connection is not dedicated in the same way as a physical tie line, which always connects the same pair of sites. In the example in Figure 20, you can use the VTLs on the Chicago system for any combination of incoming and outgoing VTL calls to either Atlanta or Dallas.

The system can reroute VTL calls that fail to reach their destination on the first attempt. For details, see "Call Rerouting for Virtual Tie Lines" on page 341.

- *You must configure the system for either IP On-the-Fly or Standard IP to use VTL connections to other systems.*
- *VTL connections are not available on a SIP-mode system.*

- *VTL connections cannot be configured to run through firewalls or NAT routers.*
- *When you calculate the number of devices on a system, do not include the number of VTLs.*

There are two implementation techniques you can use: unique extension ranges (see the next section) or site codes (see page 331).

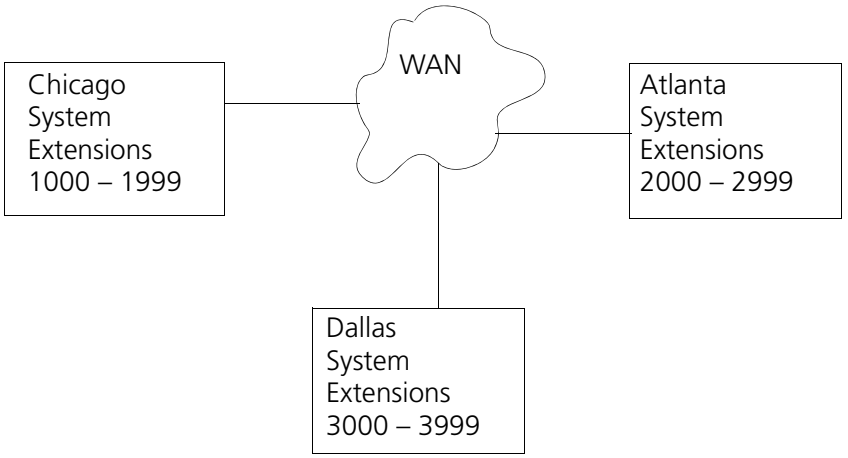
VTL Connections Using Unique Extension Ranges

If you can restrict the extension ranges on each of the systems so that they do not overlap, you can configure the dial plans to route calls based only on the extension that is being dialed. The caller does not have to dial any digits to specify the site.

Assess your growth plans for each site to verify that as you add telephones you do not exceed your defined extension ranges.

Figure 20 depicts a configuration that uses unique extension ranges.

Figure 20 Multi-site Network using Virtual Tie Lines



In the sample network shown in Figure 20, each site is set up to use a unique range of telephone extensions. The dial plan on each of the systems is configured so that whenever a call is made to an extension not located at the local site, the system sets up a VTL connection to the appropriate site.

To make a call to a user in Dallas, a user in Chicago dials a Dallas extension (3000 through 3999). The dial plan on the Chicago system is

configured to set up the necessary VTL connection to the Dallas system, and then to the extension at that site.

See "Dial Plan Configuration" on page 334 for more information about how to set up VTLs in the dial plan.

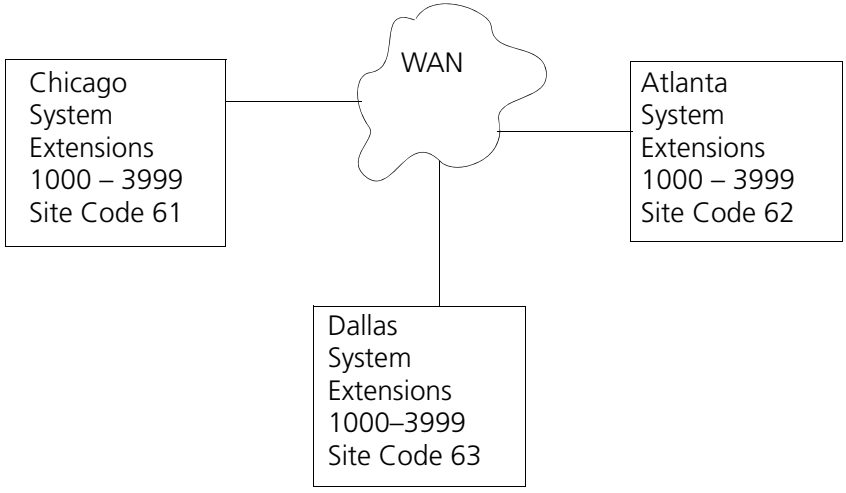
VTL Connections Using Site Codes

The simpler way to implement VTL connections uses a site code, which consists of one or more digits that a user must dial to specify the site that is being called. This approach requires no restriction on the telephone extension ranges, but does require the caller to dial the site code digits as well as the extension.

A site code can be any number of digits, but typically, one- or two-digit numbers make the most sense. The dial plan at each site must include appropriate routing instructions for each of the possible site code.

Figure 21 shows three sites connected by VTLs. All sites use the same range of extension numbers (1000 through 3999). To reach someone on another system, a user must dial a site code (61, 62, or 63 in this example) followed by an extension.

Figure 21 Virtual Tie Lines Using Site Codes



To call someone in Atlanta, a user in Chicago must dial the site code 62 and then the appropriate extension (1000 through 3999). To reach a user in Dallas, a user in Chicago must dial 63 and then the appropriate extension (1000 through 3999). Because the extension is preceded by the

site code, there is no conflict between the extension dialed and an identical extension number at the local site (Chicago). The choice of site codes is made by the person who configures the dial plans for the sites.

See "Dial Plan Configuration" on page 334 for more information about how to set up VTLs in the dial plan.

Conference Calls Using VTL Connections

Users can set up conference calls over VTLs in much the same way that they set up conference calls with other users at their local site, or at a site reachable by an external telephone line.

- On V3000, V3001R, or V5000 systems, you can have up to twelve 4-person conference calls simultaneously.
- On NBX 100 systems, you can have up to four 4-person conference calls simultaneously.

To make conference calls between sites, you must implement IGMP (Internet Group Management Protocol) on your network.

Conference Calls Using Site-Unique Extensions

In Figure 20, a user in Chicago establishes a conference call with two users in Atlanta and one user in Dallas as follows:

1. Dial the first extension in Atlanta.
2. After the user answers, press **Conference** and dial the second extension in Atlanta.
3. When the second user answers, press **Conference** again to connect all three users.
4. Press **Conference** again and dial the extension of the user in Dallas.
5. When the fourth party answers, press **Conference** to connect all four users.

Conference Calls Using Site Codes

In Figure 21, if you work in the Chicago office, to establish a conference call with two people in Atlanta and one person in Dallas:

1. Dial the site code (62) and the first extension.
2. After the first user answers, press **Conference**, dial the same site code (62) and the second extension in Atlanta.
3. When the second Atlanta user answers, press **Conference** again to connect all three users.

4 Press **Conference** again and dial the Dallas site code (63) and then the extension of the user in Dallas.

5 When the Dallas user answers, press **Conference** again to connect all four users.

Conference Calls Involving Site Codes and Off-Site Telephones

In Figure 21, you work in the Chicago office and want to establish a conference call with someone in Atlanta, someone in Dallas, and someone at an external telephone number, you:

1 Dial the Atlanta site code (62) and then the extension.

2 After the Atlanta user answers, press Conference and dial the Dallas site code (63) and then the extension.

3 When the Dallas user answers, press Conference again to connect all three users.

4 Press Conference again and dial the external telephone number.

If the site requires that you dial 9 to reach an outside telephone line, and if the call is a long-distance call, the user might dial a number in area code 367 using the digit sequence 913675551212.

5 When the person answers, press Conference again to connect all four users.

How to Configure a Virtual Tie Line

Configuring a working VTL connection between two systems involves:

- License Installation
- Dial Plan Configuration
- Updating the Extension List
- Adding VTL Devices to the Pretranslators (Optional)
- Verification of the Virtual Tie Line

You can enable silence suppression and different levels of audio compression for your VTL calls. For more information about how silence suppression and compression affect bandwidth, see "Audio Settings" on page 37. To change the system-wide settings for silence suppression and compression on VTL calls, use the NBX NetSet utility to edit the audio settings (click *System-Wide Settings* > *Audio Settings)*.

License Installation

You must obtain and install a license to enable VTLs.

Each VTL license applies only to the system on which it is installed. For example, to connect three sites by VTLs and to have each site support up to 8 simultaneous active VTL connections, install a separate license key for 8 VTLs on each of the three systems.

To increase the number of VTLs above one of the levels on a system, add one or more incremental licenses of 2 VTLs each.

To install a VTL license:

1. Click *Licensing and Upgrades* > *Licenses* > *Add License*.
2. In the field, type the license key code.
3. Click *OK* and then restart the system.

Dial Plan Configuration

You configure the dial plan after you install the VTL license. See "License Installation" on page 333 for information about VTL licenses.

To configure the dial plan for VTLs, you must define:

- Routes within the dial plan
- Digit sequences to be used to select those routes
- Operations to be performed for each route

Example: Dial Plan with Site-Unique Extensions

In Figure 20, each of the three sites uses a unique extension range. In the Internal table in the Chicago system dial plan, the entries shown in Figure 22 control the routing of calls if a user dials an extension in the 2000 through 2999 range (Atlanta extensions) or the 3000 through 3999 range (Dallas extensions) respectively. The dial plans for the Atlanta and Dallas systems would contain similar, but not identical entries.

An explanation of each line in the dial plan follows Figure 22.

Figure 22 Sample Dial Plan Entries for Chicago Using Site-Unique Extensions

```
Table Create 1 Internal 4 Digit Extensions
/                  Id Entry Digits      Min Max Class            Prio Route
/                  -- -----  ----------- --- --- -------------   ---- -----
TableEntry Create   1     3  2             4   4 WAN               0   522
TableEntry Create   1     4  3             4   4 WAN               0   523


/                       Route Description
/                       ----- -----------
DestinationRoute Create   522 Atlanta VTL Connection
DestinationRoute Create   523 Dallas VTL Connection


/                           Route Entry DestinationExtension
/                           ----- ----- --------------------
DestinationRouteEntry Create   522     1 *0006
DestinationRouteEntry Create   523     1 *0006


/                                Route Entry OperId Operation  Value
/                                ----- ----- ------ ---------  -----
DestinationRouteOperation Create   522     1      1 prepend    192*168*25*100*
DestinationRouteOperation Create   523     1      1 prepend    192*168*35*100*
```

The first *TableEntry Create* command modifies entry 3 in Table 1. Entry 3 watches for 4-digit sequences (Min = 4, Max = 4) beginning with 2 (extensions 2000 through 2999) and specifies route 522 whenever a 4-digit sequence falls within this range. Entry 4 watches for 4-digit sequences (Min = 4, Max = 4) beginning with 3 (extension 3000 through 3999) and specifies route 523 whenever a 4-digit sequence falls within this range. Route numbers 522 and 523 are examples only. The choice of route numbers is made by the person who configures the dial plans for the sites.

Two *DestinationRoute Create* commands create routes 522 and 523. The Description field contains any text you want to use to describe each route.

Two *DestinationRouteEntry Create* commands specify the extension list for routes 522 and 523. Extension list *0006 is reserved for VTLs.

Two *DestinationRouteOperation Create* commands prepend the IP Address of the destination system to the extension that the user dialed. In this example, the IP address for Atlanta is 192.168.25.100 and for Dallas, the IP address is 192.168.35.100. You must use the asterisk (*) character to separate fields within the IP address and to separate the IP address from the destination extension.

Example: Dial Plan with Site Codes

In Figure 21, each of the three sites uses the same extension range. In the Internal table in the Chicago system dial plan, the entries shown in Figure 23 select route 522 and 523 if a user dials the site codes 62 and 63 respectively, and then dials an extension. The dial plans for the Atlanta and Dallas systems would contain similar, but not identical entries.

An explanation of each line in the dial plan follows Figure 23.

Figure 23 Sample Dial Plan Entries for Chicago Using Site Codes

```
Table Create 1 Internal 4 Digit Extensions
/                  Id Entry  Digits      Min Max Class           Prio Route
/                  -- -----  ----------- --- --- -------------   ---- -----
TableEntry Create   1   100  62            6 6   WAN             0    522
TableEntry Create   1   101  63            6 6   WAN             0    523


/                      Route Description
/                      ----- -----------
DestinationRoute Create   522 Atlanta VTL Connection
DestinationRoute Create   523 Dallas VTL Connection


/                           Route Entry DestinationExtension
/                           ----- ----- --------------------
DestinationRouteEntry Create   522     1 *0006
DestinationRouteEntry Create   523     1 *0006


/                               Route Entry OperId Operation  Value
/                               ----- ----- ------ ---------  -----
DestinationRouteOperation Create   522     1      1 stripLead  2
DestinationRouteOperation Create   522     1      2 prepend    192*168*25*100*
```

The first *TableEntry Create* command creates entry 100 in Table 1. This assumes that the highest previous entry in Table 1 was 99 or lower. Entry 100 watches for the 2-digit sequence 62 followed by a 4-digit extension and specifies route 522 whenever a user dials such a 6-digit (Min = 6 and Max = 6) sequence. Entry 101 watches for the 2-digit sequence 63 followed by a 4-digit extension and specifies route 523 whenever a user dials such a 6-digit sequence. The choice of route numbers is made by the person configuring the dial plans for the sites.

Two *DestinationRoute Create* commands create routes 522 and 523. The Description field contains any text you want to use to describe each route.

Two *DestinationRouteEntry Create* commands specify the extension list for routes 522 and 523. Extension list *0006 is the default extension list for VTLs.

For each DestinationRoute, two *DestinationRouteOperation Create* commands perform two functions:

- The *stripLead* command removes the two digits (62 or 63) leaving the 4-digit extension the user dialed.
- The *prepend* command adds the IP Address of the destination system to the extension that the user dialed. In this example, the IP address for Atlanta is 192.168.25.100 and for Dallas, the IP address is 192.168.35.100. In the dial plan, you must use an asterisk (*) instead of a period (.) to separate the fields within the IP address, and to separate the IP address from the destination extension.

Updating the Extension List

The final step to activate the virtual tie lines is to add the VTL extensions to the appropriate extension list (*0006).

To update the extension list:

1. Log on to NetSet using the administrator login ID and password.
2. Click *Dial Plan > Extension Lists*.
3. Click **0006*, which is the Virtual Tie Lines extension list.

   The system displays the Modify window, which includes a membership list. The membership list can list the members already added to the VTL extension list, or a full listing of extensions if the extension list has no members.

4 To add an extension to the list:

c If the list does not include any members, click the check boxes next the extension of the VTL that you want to add to the list.

d If the list already has members, click *Show all* to display a list of extensions that you can add to the list's membership.

***Note**: You can toggle between the **Show all** and **Show members only** buttons to display extensions that have membership in the extension list and the extensions that are not members of the list but which you can add to the list, and to confirm your changes.*

The system displays *(VTL)* and the name of the virtual tie line in the Device Description field. The number of VTL extensions depends on the VTL license installed on this system. Table 61 describes the VTL extension ranges.

Table 61 Virtual Tie Line Extension Ranges

Platform	Extension Range
V3000 4-digit dial plan	6500–6523
V3000 3-digit dial plan	The default dial plan for a V3000 system is 4-digit. If you convert to a 3-digit dial plan, you must manually change each 4-digit extension to a 3-digit extension. For VTLs, you can select any unused 3-digit extension from the external extension range (600–799).

Adding VTL Devices to the Pretranslators (Optional)

If you add a VTL pretranslator to the dial plan to reformat the information of incoming VTL calls, you *must* add the VTL devices to that pretranslator. You can add a pretranslator to the dial plan to format caller ID and CDR records for VTL calls. See "Creating a Pretranslator for VTL Calls" on page 297.

To add the VTL devices to the pretranslator:

1 Log on to NetSet using the administrator login ID and password.

2 Click *Dial Plan* > *Pretranslators*.

3 Click the VTL pretranslator.

4 In the *Devices Using* window, click the check boxes next to the devices associated with VTLs. For a 4-digit dial plan, the VTL device extensions range from 6500 through 6523. For a 3-digit dial plan, VTL device extensions range from 623 through 630.The device descriptions include *(VTL)*.

5 Click *OK*.

Verification of the Virtual Tie Line

After you have configured the VTLs on each of two systems, verify that the VTL connection works properly.

To verify that a working VTL connection exists between two systems, you must verify:

- Local System Verification — Verify that the configured VTLs appear on each system.
- Remote Access Verification — Verify that each of the systems can access each other.
- Placing Telephone Calls — Verify that telephone users can make calls can between all pairs of connected systems in both directions.

Local System Verification

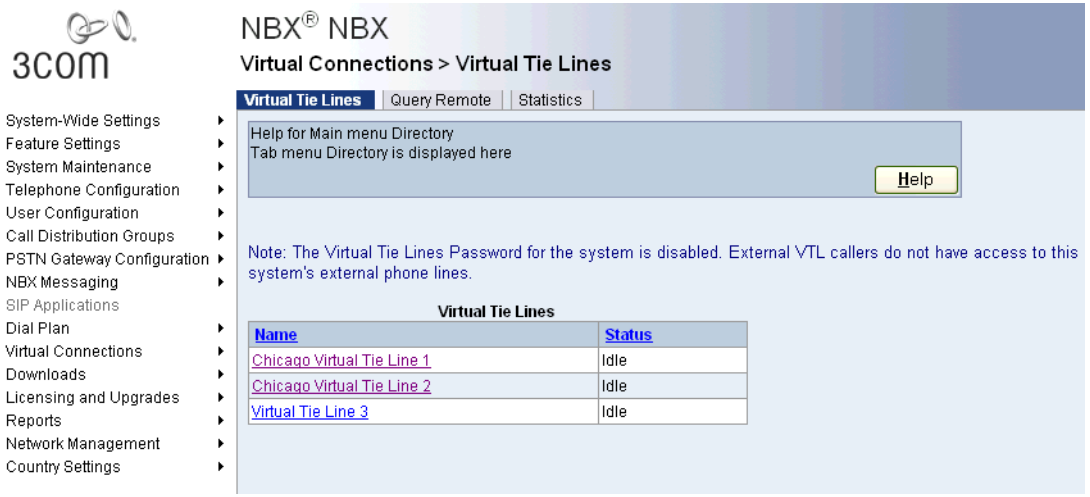
On each system, use the NBX NetSet utility to verify that you can view the local VTLs:

1 Click *Virtual Connections* > *Virtual Tie Lines*.

2 Verify that the list displays the VTLs you configured.

In our example, if you perform this verification test on the Chicago system, the results appear as shown in Figure 24.

Figure 24 Example: Virtual Tie Lines Window



Remote Access Verification

To verify that each system can access the other, on each system:

1. Click *Virtual Connections* > *Virtual Tie Lines*.
2. Click the *Query Remote* tab.
3. In the *Query Remote* window, type the IP address of the remote system in the *IP address* field and click *Query*.

   If the verification is successful, the window displays the VTLs configured at the remote site.

   Example: You have installed an system in Chicago, Atlanta, and Dallas, and you have configured two VTL connections on each of the Chicago and Atlanta systems. The IP addresses of the three systems are:

   - Chicago — 192.168.15.100
   - Atlanta — 192.168.25.100
   - Dallas — 192.168.35.100

   The Atlanta system (IP address 192.168.25.100) shows two installed but idle VTL connections. If you execute the Query Remote operation from the Atlanta office and specify the IP address of the Chicago system, the local system displays two installed but idle VTL connections.

   If the local system fails to access the remote system, it displays an error message.

   If you have not yet configured the remote system to support VTLs, this message indicates that you must do so before the Query Remote operation can succeed.

   If you have configured the remote system to support VTLs, the error message indicates that the local system cannot access the remote system using the IP address you specified. To correct the problem:

1. Verify that you specified the correct IP address for the remote system.
2. Verify that the remote system is running properly.
3. Verify that the remote system is using the dial plan which you modified to configure VTLs on that system.
4. Work with your network administrator to verify that WAN connection between the two sites is properly configured and is working.
5. Verify that the VTL extensions are included in the *Devices Using Pretranslator* table.

Placing Telephone Calls

The final step to verify a virtual tie line connection is to place telephone calls in both directions between each pair of connected sites.

Call Rerouting for Virtual Tie Lines

To enable the system to better deal with network problems, you can configure the system dial plan so that some virtual tie line (VTL) calls can be rerouted if a VTL connection cannot be made.

VTL calls can be rerouted if:

- The dial plan contains an invalid IP address
- The remote system is not responding
- All VTL channels on the remote system are currently busy
- All IP addresses in the IP On-the-Fly address pool are in use

Some VTL calls are not rerouted. Example situations in which a call is not rerouted include:

- Placing a VTL call to another system with the intention of hopping off (dialing a telephone number local to the other system) when all trunks are busy on the other system
- Dialing an invalid telephone number

If you normally connect calls from site A to site B using VTL connections, you can define an alternate route to site B using Analog Line Card ports, Digital Line Card channels, etc. If a network problem such as a router failure occurs, or if all VTL ports on the site A system are busy, VTL calls that fail to reach site B are then dialed using the alternate route.

If your VTL call is rerouted, you see additional routing information in the display panel on your telephone.

The system log file contains records of failed VTL calls that were rerouted.

Example Dial Plan Entries

If you normally dial a site code such as 72 to reach site B, and if the telephones at the other site use four-digit extensions, the dial plan entries to manage the initial call and the rerouting of the call might look like the example shown in Figure 25.

Figure 25 Sample Dial Plan Entries for Rerouting VTL Calls

```
Table Create 1 Internal 4 Digit Extensions
/                  Id Entry  Digits       Min Max Class           Prio Route
/                  -- ------ ------------ --- --- -------------   ---- -----
TableEntry Create   1      8 72             6   6 WAN                0     6



/        Routes
/                       Route Description
/                       ----- -----------
DestinationRoute Create     6 Site B



/                           Route Entry DestinationExtension
/                           ----- ----- --------------------
DestinationRouteEntry Create     6     1 *0006
DestinationRouteEntry Create     6     2 *0001



/                                Route Entry OperId  Operation  Value
/                                ----- ----- -------  ---------  -----
DestinationRouteOperation Create     6     1       1 stripLead  2
DestinationRouteOperation Create     6     1       2 prepend    192*168*155*100*
DestinationRouteOperation Create     6     2       1 stripLead  2
DestinationRouteOperation Create     6     2       2 prepend    1978247
```

Explanation:

The TableEntry Create command specifies that when a user on the local system dials a six-digit number beginning with the digits 72, the call is routed via route 6, which is the route that normally contains only the VTL extension list (*0006).

To allow VTL calls to be rerouted, route 6 is configured to use both the VTL extension list and the Line Cards extension list (*0001). Calls that use route 6 can be completed using devices in either of these extension lists.

There are four DestinationRouteOperation lines. The first two lines specify the primary way to manage the call, using VTL methods. The last two lines specify the backup way to manage the call if the first method fails.

Successful VTL Call

If there are no network problems:

1. The first line (Entry 1, OperId 1) removes the digits 72.
2. The second line (Entry 1, OperId 2) prepends the IP address of the system at site B in front of the dialed extension number.

Unsuccessful VTL Call

If a network problem or a lack of VTL ports prevents the VTL call from reaching its destination:

1. The third line (Entry 2, OperId 1) removes the digits 72.
2. The fourth line (Entry 2, OperId 2) prepends an appropriate dial string and dials out over an analog telephone line.

Managing Existing Virtual Tie Lines

After VTLs are installed and you have verified that they are working properly, you can manage them using the NBX NetSet utility. There are NetSet utility functions for:

- Modifying a Virtual Tie Line Name
- Viewing and Resetting Virtual Tie Line Statistics
- Enabling Audio Compression for VTL Calls
- Enabling Silence Suppression on VTL Calls

Modifying a Virtual Tie Line Name

You can change the name of a VTL. The name appears in NetSet lists, and helps you identify each VTL.

To modify the name of a VTL:

1. Click *Virtual Connections* > *Virtual Tie Lines*, which displays the list of existing VTLs, and the status of each one.
2. Select a VTL from the list, which displays the Modify window.
3. In the *New VTL name* field, type the name you want to assign to this VTL.
4. Click *OK* and verify the name change is in the Virtual Tie Lines window.

Viewing and Resetting Virtual Tie Line Statistics

You can view the statistics for a VTL at any time.

To view statistics for a VTL:

1 Click *Virtual Connections* > *Virtual Tie Lines*.

2 Click the *Statistics* tab, which displays the Statistics window and the information described in Table 62.

3 To reset all VTL statistics, click *Reset*.

If you restart the system, it resets all VTL statistics.

Table 62 Virtual Tie Line Statistics Fields

Field	Description
NOTE: All statistics apply to the time period since the most recent Reset command or since the most recent system reboot, whichever was more recent. To determine the starting time for the displayed statistics, compare the *Last reset command* with the time of the *Last system reboot*. Both are displayed at the bottom of the VTL Statistics window.	
Number of outgoing VTL calls made	The number of outgoing calls made over all virtual tie lines (VTLs) since the most recent reset command or since the time the system was last restarted. Each time you restart the system, you reset the statistics for all VTLs.
Number of incoming VTL calls received	The number of incoming calls received over all VTLs since the most recent reset command or since the time the system was last restarted.
Number of active VTL calls	The number of calls currently active on all VTLs.
Maximum number of concurrently active VTL calls	The maximum number of VTL calls that have been active at the same time on this system since the most recent reset command or since the time the system was last restarted.
Incoming VTL calls rejected due to all VTLs busy	The number of telephone calls that would have arrived from other systems over VTL channels, but could not be accepted because all local VTL ports were busy when the calls arrived.
Outgoing VTL calls rejected due to all VTLs busy	The number of telephone calls that would have been sent from the local system over VTL channels, but could not be sent because all local VTL ports were busy when the calls were made.
Rerouted VTL calls	The number of calls that did not reach their destination when attempted over VTL channels, and were rerouted using another device.
Last reset command	The date and time of the most recent *Reset* for this VTL.
Last system reboot	The date and time of the most recent reboot of the system.

Enabling Audio Compression for VTL Calls

You can set audio compression for VTL calls. The default condition is no audio compression because compression can compromise audio quality.

For more information about how compression affects bandwidth, see "Audio Settings" on page 37.

During VTL call setup, the VTL software at each end of the call negotiates a compression level that is supported by both systems. For example, System A is configured for G729, high compression, and System B is configured for G711, no compression. A VTL call between System A and System B will use G711, no compression. It does not matter which system initiates the call.

To enable VTL audio compression:

1. Click *System-Wide Settings* > *Audio Settings*.
2. Click the *Audio Compression on VTL Calls* check box and then click *OK*.

Enabling Silence Suppression on VTL Calls

You can enable silence suppression for VTL calls. The default condition is disabled because silence suppression can compromise audio quality. For more information about how compression affects bandwidth, see "Audio Settings" on page 37.

When you enable VTL silence suppression, the VTL software attempts to use silence suppression on all VTL calls. If the other system is not configured to support silence suppression, the local VTL software attempts to find a compatible communications mode.

Do not enable silence suppression unless you have network congestion problems you cannot solve otherwise. Enabling silence suppression can reduce network traffic, but the result is a compromise to audio quality.

To enable silence suppression on VTLs:

1. Click *System-Wide Settings* > *Audio Settings*.
2. Under *VTL Audio Calls Settings*, enable the *Enable Silence Suppression* check box.
3. Click *OK*.

Using a VTL Password

To allow users on one system to place VTL calls to another system and then place long-distance (toll) calls from that location (a practice called 'hop off'), you can configure a VTL password.

When an system receives a VTL call from a user on another system, it can allow that user to make long-distance calls if the incoming VTL call

contains the password. Otherwise, such calls are not allowed. If you set up two classes of VTL calls (with and without passwords), you can permit or deny hop off.

To enable a system to manage incoming hop off calls, create or modify a VTL password, as described in the next topic, Configuring a VTL Password.

To enable a system to send hop off VTL calls, configure the dial plan to include the VTL password, as described in Configuring VTL Passwords in the Dial Plan on page 346.

Configuring a VTL Password

For each system that can receive VTL calls, use the NBX NetSet utility to configure a local system VTL password.

To configure the password:

1. Click *System Maintenance* > *Password Administration*.
2. Select *Virtual Tie Lines Password* in the *Password* list, and then click *Go*.
3. Type the administrator password in the *Current Admin Password* field.
4. Type the new VTL password in the *New Virtual Tie Lines Password* field.

Passwords are from 8 to 15 characters in length and must contain only letters and numbers. Upper and lower case letters are permitted.

5. Retype the new VTL password in the *Re-enter New Password* field.
6. Click *OK*.

Configuring VTL Passwords in the Dial Plan

For each remote system that controls hop-off by means of a VTL password, configure that password into the VTL commands in the local dial plan.

If you use site codes to access other systems through VTL connections, you can configure one set of VTL connections that permit hop-off and are accessed by one set of site codes. You can configure another set of VTL connections that do not permit hop-off and are accessed using a different set of site codes.

If you use unique extension ranges at each site, and therefore do not dial a site code when placing VTL calls to users at those sites, you can still use codes to access VTL connections that permit hop-off at the far end.

Figure 26 shows how to configure VTL passwords in a dial plan, using site codes that permit hop-off and other site codes that do not.

Figure 26 Dial Plan Entries for VTL Passwords

```
Table Create 1 Internal 4 Digit Extensions
/                  Id Entry  Digits      Min Max Class            Prio Route
/                  -- -----  ----------- --- --- -------------    ---- -----
TableEntry Create   1   100  62            6 6   WAN              0    522
TableEntry Create   1   101  63            6 6   WAN              0    523
TableEntry Create   1   102  72            6 32  WAN              0    524
TableEntry Create   1   103  73            6 32  WAN              0    525


/                       Route Description
/                       ----- -----------
DestinationRoute Create   522 Atlanta VTL Connection
DestinationRoute Create   523 Dallas VTL Connection
DestinationRoute Create   524 Atlanta VTL Connection with password
DestinationRoute Create   525 Dallas VTL Connection with password


/                            Route Entry DestinationExtension
/                            ----- ----- --------------------
DestinationRouteEntry Create   522     1 *0006
DestinationRouteEntry Create   523     1 *0006
DestinationRouteEntry Create   524     1 *0006
DestinationRouteEntry Create   525     1 *0006


/                                Route Entry OperId Operation  Value
/                                ----- ----- ------ ---------  -----
DestinationRouteOperation Create  522    1     1  stripLead 2
DestinationRouteOperation Create  522    1     2  prepend   192*168*25*100*
DestinationRouteOperation Create  523    1     1  stripLead 2
DestinationRouteOperation Create  523    1     2  prepend   192*168*35*100*
DestinationRouteOperation Create  524    1     1  stripLead 2
DestinationRouteOperation Create  524    1     2  prepend192*168*25*100*ATLPassW*
DestinationRouteOperation Create  525    1     1  stripLead 2
DestinationRouteOperation Create  525    1     2  prepend 92*168*35*100*DALPWord*
```

The first *TableEntry Create* command creates entry 100 in Table 1. This assumes that the highest previous entry in Table 1 was 99 or lower. Entry

100 watches for the 2-digit sequence 62 followed by a 4-digit extension and specifies route 522 whenever a user dials such a 6-digit (Min = 6 and Max = 6) sequence. Entry 101 watches for the 2-digit sequence 63 followed by a 4-digit extension and specifies route 523 whenever a user dials such a 6-digit sequence. The choice of route numbers is made by the person configuring the dial plans for the sites.

The next two *TableEntry Create* commands are set up in a similar manner to manage VTL connections with passwords. If a user dials 72 followed by a 4-digit extension, the VTL call uses route 524. If a user dials 73 followed by a 4-digit extension, the VTL call uses route 525. These two commands specify a minimum of 6 digits (for example, if the caller is calling an internal extension preceded by the site code) and a maximum of 32 digits (for example if the caller is calling a long-distance or international number preceded by the site code).

The first two *DestinationRoute Create* commands create routes 522 and 523. The Description field contains text that describes each route.

The second two *DestinationRoute Create* commands create routes 524 and 525, the routes that are used with a VTL password.

The four *DestinationRouteEntry Create* commands specify the extension list for routes 522, 523, 524, and 525. Extension list *0006 is the default extension list for VTLs.

For the first two DestinationRoutes, two *DestinationRouteOperation Create* commands perform two functions:

- The *stripLead* command removes the two digits (62 or 63) leaving the 4-digit extension the user dialed.
- The *prepend* command adds the IP Address of the destination system to the extension that the user dialed. In Figure 26, the IP address for Atlanta is 192.168.25.100; for Dallas, 192.168.35.100. In the dial plan, use an asterisk (*) instead of a period (.) to separate the fields within the IP address, and to separate the IP address from the destination extension.

For the second two DestinationRoutes, two DestinationRouteOperation Create commands perform two similar functions.

- The *stripLead* command removes the two digits (72 or 73) leaving the 4-digit extension the user dialed.

- The *prepend* command adds the IP address and system password of the destination system to the extension dialed by a user. In Figure 26, the IP address for Atlanta is 192.168.25.100 and the password is ATLPassW. For Dallas, the IP address is 192.168.35.100 and the password is DALPWord. In the dial plan, you use an asterisk (*) instead of a period (.) to separate fields within the IP address and to separate the IP address from the destination extension.

To place a hop-off call to 555-1212 in area code 903 through the Atlanta system, a user on a remote system would dial 72919035551212. The 72 code sets up a VTL connection to Atlanta that incudes the Atlanta system's VTL password, and the remaining digits are used to dial the number (9 accesses an outside line to obtain dial tone from the local carrier, 1 accesses the long-distance carrier, and the remaining digits specify the long-distance number).

If the same user used site code 62 to place a call to the Atlanta office, only toll-free, emergency, and internal call would be allowed.

Toll Calls Without a VTL Password

If a local user has configured his telephone to forward calls to a long-distance number, then an incoming VTL call to that telephone does not need to supply the local system's VTL password in order for the call to be forwarded.

Music On Hold

If two users are talking on a VTL connection, and the first user places the call on hold, the second user hears Music On Hold only if his local system is configured to play it.

Troubleshooting VTL Calls

Table 63 contains a list of error situations, the possible causes and the action to take in each case.

Table 63 VTL Errors and Corrections

Error Condition	Possible Causes	Actions
Long pause after dialing. Telephone display contains "VTL" during the pause. Busy signal is then heard.	Remote server does not respond	Test the connection to the remote system using the Query Remote function.

Table 63 VTL Errors and Corrections (continued)

Error Condition	Possible Causes	Actions
After you dial a VTL call, there is a busy signal and the telephone display panel displays the "All ports busy" message.	1. No VTL license installed. 2. VTL device extensions not added to Extension List *0006. 3. All local VTL connections are currently in use. 4. All VTL connections at the remote site are currently in use.	1. Verify that the licenses appear when you access the tab. 2. Verify that the *0006 extension contains the VTL device extensions. 3. On the Virtual Tie Line tab, verify that there is at least one idle VTL connection. 4. Use the Query Remote function to verify that there is at least one idle VTL connection.
After you dial a VTL call, there is a busy signal and the telephone display panel displays the "Invalid Number" message.	1. Local dial plan is not properly configured. 2. Dial plan on the remote (target) system in not properly configured. 3. You are trying to use hop-off without the necessary password.	1. Examine the local dial plan for errors. 2. Examine the dial plan on the remote system for errors. 3.Verify that the password for the remote system is used in both dial plans.
No audio	1. Telephones are not configured to use either IP On-the-Fly or Standard IP. 2. VTL Audio compression is supported on only one of the two systems. 3. 3C10165D E1 and 3C10116D T1 Digital Line Cards do not have static IP addresses.	1. Verify that the IP setting in the System Settings, System-Wide dialog box is "IP On-the-Fly" or "Standard IP." Change the setting, if necessary. 2. Verify that audio compression is enabled on both systems. 3. If your system is set up for IP On-the-Fly, verify that 3C10165D E1 and 3C10116D T1 Digital Line Cards have a static P address. These cards cannot receive an IP On-the-Fly address.
Caller ID information does not display correctly in the telephone display panel.	1. Invalid local pretranslator. 2. VTL extensions are not in the VTL pretranslator "Devices Using" table.	1. Examine the local dial plan for pretranslator errors. 2. Verify that VTL extensions appear in the left-hand table for the pretranslator.

TAPI Route Points

A TAPI Route Point is a virtual device within the system where calls are held pending action by an external TAPI application. Route points are typically used by call center applications to redirect calls. A redirected call is one that is sent from its original destination (the route point) without being answered, to a new location specified in the external application.

A TAPI Route Point in the system is an extension with a voice mailbox in the normal extension range:

- **V3000, V3001R, V5000 systems:** 1000 – 3999
- **NBX 100 systems:** 100 – 449

You create the TAPI Route Point, configure the system to route calls to it, and then configure the external application to monitor it. For example, you can configure a line card port to send all incoming calls on that line to a specific TAPI Route Point. When a call arrives at the route point extension, it is queued until the external application examines it and then instructs the Call Processor to redirect the call to a destination specified in the external application. Typically, the redirect action is based on the caller ID information of the incoming call.

Redirect Behaviors

Table 64 describes the behavior of TAPI Route Points and redirected calls within the system.

Table 64 TAPI Route Points and System Features

Call Redirected to	Description
Internal extension	If the internal extension has activated Do Not Disturb, a call redirected to that extension goes immediately to the extension's Call Forwarding setting. If the TAPI Line Redirect Timeout is set to a value greater than the extension's Call Forwarding setting and the call is not answered, the redirected call will be managed by the extension's Call Forwarding setting. The system will log a successful redirect. If the TAPI Line Redirect Timeout is set to a value less than the extension's Call Forwarding setting and the call is not answered, the call will return to the route point. For more information, see "Specifying TAPI Line Redirect Timeout" on page 354.

Table 64 TAPI Route Points and System Features (continued)

Call Redirected to	Description
External number	Subject to the route point extension's Class of Service setting.
	The call connects as soon as the external line resource (line card port, a PRI line, or a T1 channel) is acquired. The caller hears the call progress tones directly from the CO. At this point, the system logs a successful connection. Calls redirected to an external number cannot timeout, even if the call was redirected to a busy or an invalid number.
Call Park extension	If a call has been previously parked at the specified Call Park extension, the redirected call is connected to the parked call.
	If no call is waiting at the specified Call Park extension, the call returns to its original destination when the TAPI Line Redirect Timeout expires and the external application can redirect it again. After two failures, the call goes to the Call Coverage specified for the Route Point.
Hunt Group extension	Calls redirected to a Hunt Group extension do not timeout. Once the call is passed to the Hunt Group, the system reports that the call has been successfully redirected.
	Calls can be redirected from a Hunt Group extension.
	You cannot add a TAPI Route Point extension to a Hunt Group.
Hunt Group member	A Hunt Group takes precedence over a Route Point. If a call arrives on a Hunt Group member telephone because it is a member of a Hunt Group, a redirect is not permitted. If a call arrives on the phone's extension (not as a result of a Hunt Group action), the call can be redirected.
Phantom Mailbox	A call can be redirected to a phantom mailbox.
Mapped Line	Calls that arrive through an incoming line that is mapped to a line appearance button on a telephone cannot be redirected.
	If you redirect a call to a mapped line, the call does not timeout. It fails and is routed back to the route group until the caller disconnects.
Bridged Station Appearance	Calls can be redirected to or from a telephone that has a bridged station appearance. Once a call to a primary bridged station appearance reaches the secondary bridge station appearance, the call cannot be redirected.
Configurable Operator	Calls can be redirected to a System Operator or a Personal Operator.

TAPI Route Point Capacities

When the maximum number of calls on a route point is reached (see Table 65), subsequent calls routed into the route point from an internal extension or through a Virtual Tie Line ring for 10 seconds and are then disconnected. If the call arrives through a line card port, the call continues ringing.

Table 65 TAPI Route Point Capacities

System	Maximum Number of Route Points	Maximum Number of Calls per Route Point
NBX 100, V3000, V3001R, V5000	100	400
NOTE: A 3-digit dial plan might not provide enough extensions to support 100 TAPI Route Points.		

Creating a TAPI Route Point

To create a new TAPI Route Point, the system administrator performs these steps:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *Virtual Connections* > *TAPI Route Points*.
3. Click *Add* to open the Add TAPI Route Point window.
4. Enter the appropriate information in the fields.
5. See the see the online Help for more information.

Modifying a TAPI Route Point

To modify a TAPI Route Point:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *Virtual Connections* > *TAPI Route Points*.
3. From the list of TAPI Route Points, select the one you want to modify to open the Modify window.
4. See the see the online Help for more information.

To modify the password for the TAPI Route Point, enter the administrator password for the system in the Current Admin Password *field.*

Viewing TAPI Route Point Statistics

You can view the statistics for all of the TAPI Route Points on this system. The system starts to accumulate new statistics each time you reboot the

system or each time you click the *Reset* button in the TAPI Route Point Statistics dialog box.

To view TAPI Route Point statistics:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *Virtual Connections* > *TAPI Route Points* tab.
3. Click the *Statistics* button.
4. Click the heading of any column to sort the data in ascending or descending order.
5. Click *Reset* to erase all data. The system begins collecting new statistical data.

   The *Last reset command* field displays the date and time of the most recent Reset. A row of hyphens (----------) indicates no Reset since the most recent system reboot.

   The *Last system reboot* field contains the date and time when the system was most recently rebooted.

   See the online Help for information about dialog box fields.

Specifying TAPI Line Redirect Timeout

The TAPI Line Redirect Timeout is a system-wide timer that specifies the amount of time before a redirected call goes back to its original destination, which allows the TAPI application to redirect the call again. When a redirected call times out, the system also sends a failure code back to the TAPI application. After two failures, the call goes to the route point's call coverage option.

To set the TAPI Line Redirect Timeout:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *System-Wide Settings* > *Timers.*
3. See the online Help for the procedure to set timers.

TAPI Supervisory Monitoring

You can configure the system to allow a privileged user to join an ongoing conversation with or without the knowledge of the parties involved in that conversation. This feature is called *Supervisory Monitoring*.

The monitoring user is called the *supervisor*. The supervisor, who might or might not be the system administrator, can join a call between a person calling into the system (for example, a customer) and a person on-site whose job it is to accept incoming calls. Joining calls in progress can ensure proper customer support.

The system allows Supervisory Monitoring on outgoing calls as long as the agent is in the domain that corresponds to the password that the supervisor uses to monitor the agent.

To use Supervisory Monitoring, the supervisor needs:

- The Route point extension
- The Supervisory Monitoring Domain password
- The agent's telephone extension

To set or change the Supervisory Monitoring password, you need first to provide the system administrator password. The System Administrator configures Supervisory Monitoring parameters using the *Supervisory Monitoring* window of the NBX NetSet utility.

Supervisory Monitoring uses IP Multicast. Because the system has a global pool of multicast addresses that Supervisory Monitoring and other features use, it is possible for the system to exhaust its pool of multicast addresses and thus return an error to a monitoring request.

Supervisory Monitoring Modes

This section describes the different modes that a supervisor can employ to monitor incoming calls.

As a supervisor, you can employ Supervisory Monitoring in any of the following modes:

- **Monitor**

  Allows you to join a call in progress without an alert that is audible by either the agent or the customer.

  Monitor mode requires a password. To start monitoring a call, the supervisor must use one of the following:

  - Feature code **425**
  - Mapped button
  - Display panel Soft Key (not available on all phones) that the administrator has configured for this purpose.

- **Whisper** (also known as **Coaching**)

  Allows you to join a call in progress to speak with the agent without alerting the customer to your presence. **Whisper** mode requires a password.

- **Barge-In**

  Allows you to join a call in progress to speak with both the agent and the customer. **Barge-In** mode requires a password.

Either the agent or the supervisor can put the call on hold while Supervisory Monitoring is in effect. This means that the supervisor can initiate two monitoring sessions: one active session and one on hold.

TAPI Settings

You must configure system-wide Telephony Application Programming Interface (TAPI) settings before users can download the NBX TAPI Service Provider (NBXTSP). NBXTSP enables a TAPI application on a user's PC to interact with the user's 3Com telephone. You can set a maximum number of TAPI clients in the system. You can also require users to enter passwords for TAPI devices.

Before you configure system-wide TAPI settings, install the appropriate TAPI software. After you have the software installed, select *Virtual Connections > TAPI Settings* to configure TAPI settings. See the online Help for procedures to configure TAPI settings and download NBX TSP software.

The TAPI settings do not apply to TAPI Route Points. For security reasons, the system always requires that an external application supply a password to access a TAPI Route Point.

13 DOWNLOADS

This chapter provides information about downloading:

- Software
- LabelMaker
- Documentation and Reference Guides

For more information about these topics and configuration procedures, see the online Help.

Software

You can download these applications:

- **NBX Call Reports** — You can install NBX® Call Reports on a computer that runs the Microsoft Windows 2000 or Windows XP operating system. The application enables you to retrieve call logging information from the system for reporting purposes. See Chapter 15 for prerequisites and details on running these reports.
- **NBX TAPI Service Provider (NBX TSP)** — You can install NBX TSP on a computer that runs the Microsoft Windows 2000 or Windows XP operating system. The application enables you to use TAPI-enabled programs with the system. For more information, see Chapter 2.
- **3Com Telephone Local Configuration Application** — You can install the application on a computer that runs the Microsoft Windows 2000 or Windows XP operating system. Devices with a display panel use the Local User Interface (LUI) to define the settings that the device needs to communicate with the Call Processor. For telephones that do not have a display panel, such as the 3Com 3100 Entry Telephone, use the Telephone Local Configuration (TLC) application to define these settings. See Chapter 18 for more information about how to configure devices.

To download software applications, click *Downloads* > *Applications* and see the online Help for more information.

LabelMaker

Each 3Com Telephone and Attendant Console comes with a set of blank labels on which users and administrators can write Speed Dials and other unique settings that have been applied to the buttons. If you are setting up many telephones with similar features, you can use the LabelMaker utility to create and print your labels.

Users and administrators launch the same LabelMaker. The LabelMaker utility can create labels for all 3Com telephones and Attendant Consoles.

The LabelMaker is a Windows program file. If you use an operating system that cannot run Windows programs, contact your 3Com NBX Voice-Authorized Partner for a PDF version of the LabelMaker.

To launch the LabelMaker and select a label:

1. Log in to the NBX NetSet utility using the administrator username and password.
2. Click *Downloads* > *LabelMakers* > *Universal LabelMaker*.

   You can also log in as a user and click *Resources* > *Telephone Button Labels* to launch the LabelMaker.
3. See the online help for more information about how to create and print labels.

Documentation and Reference Guides

You can view and download Adobe PDF versions of the following guides:

- *NBX Installation Guide*
- This administrator's guide
- Telephone guides for 3Com telephones
- *NBX Feature Codes Guide for Analog Telephones*
- *NBX Feature Codes Guide for SIP Telephones*
- *IP Messaging Module Installation Guide*

To view and print the documentation, click *Downloads* > *Documentation*.

Telephone users can click *Resources* and then the appropriate tabs to access quick reference guides, telephone guides, and the feature codes guide.

You can get or upgrade your existing version of Adobe Acrobat Reader from the Adobe web site, www.adobe.com.

14 LICENSING AND UPGRADES

This chapter describes how to manage licensing and upgrade operations for your system. It describes:

- Licenses
- Software Upgrade
- Third-Party Drivers

For more information about these topics and configuration procedures, see the online Help.

Licenses

You can install licenses on your system for these components:

- System software
- 3Com ConneXtions H.323 Gateway
- pcXset™ (Soft Telephone) application
- Voice mail (Additional voice mail and Auto Attendant ports and voice mail storage)
- Disk mirroring (V5000 and V3001R systems only)
- Devices (specifies the total number of devices allowed on the system)
- Windows Audio Volume (WAV) devices
- Virtual Tie Lines (VTLs)
- Internet Voice Messaging (VPIM)
- Third-Party Messaging
- Complement Attendant Software
- Call Recording & Monitoring
- Polycom Telephones
- Legacy Link Nortel, Meridian, and Analog Telephones

- Groups 0 – 4 Devices
- Automatic Call Distribution (ACD)

See the *NBX Installation Guide* for a complete list of licenses and system capacities.

To manage your software licenses:

1. Login to the NBX NetSet utility using the administrator login ID and password.
2. Click *Licensing and Upgrades > Licenses*.
3. See the online Help for procedures to manage licenses.

Add a License

Each system includes a factory default license associated with the system serial number.

- On V3000 and V3001R systems, the serial number is on the front of the chassis.
- On V5000 systems, the serial number is on the disk tray.
- On NBX 100 systems, the serial number is on the Call Processor backplane.

To configure the system to support new licenses, contact your 3Com dealer and provide the serial number. The dealer obtains a new license key from 3Com Customer Support that enables the upgrade.

See the online Help for procedures to add a license to a system.

Remove a License

The only license that you can remove from a system is the disk mirroring license, which enables a V5000 or V3001R system to use two disks in a mirrored configuration.

CAUTION: *See "Reverting to a Single-Disk System" on page 91 for instructions how to remove the disk mirroring license. If you do not follow the procedure correctly, you might not be able to restart the system.*

The system displays the Remove License button on V5000 or V3001R systems only.

Usage Report

For each license installed on the system, the Usage Report displays the current number of devices in use for the license type and the maximum number of devices allowed by that license.

Backing Up Licenses

3Com recommends that you make a backup copy of all licenses on your system.

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *Licensing and Upgrades* > *Licenses.*
3. Click *Backup.*
4. Click *Save*, choose a location to save the backup file, and click *Save* again.

You can also back up licenses if you click System Maintenance > System Backup *and enable the* Include NBX Licenses *check box.*

Restoring Backed-Up Licenses

You can restore all licenses from a previously created backup file.

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *Licensing and Upgrades* > *Licenses*.
3. Click the Restore Licenses tab.
4. Type the full path to the license backup file in the *Enter path to restore license(s) on this system:* field or browse to the location in which you saved the licenses backup file.
5. Click *Restore* and respond to the confirmation prompt message that appears.

   ***NOTE**: After you restore the licenses, you must restart the system. Therefore, 3Com recommends that you restore licenses only during non-business hours.*

Obtaining Details of License History

You can view a detailed history, including the date and time on which each license was added to the system.

To view the license detail report, click *Licensing and Upgrades* > *Licenses* > *License Details*.

Software Upgrade

As part of the upgrade and reboot process, you can choose to use your existing configuration data with the new version of the software or use a new (empty) database. the NBX NetSet utility allows you to choose which software version to use when you reboot the system. This allows you to restore an earlier operating environment (both software and configuration data), if necessary.

To upgrade or remove software:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *System Maintenance* > *System Software Upgrade*.
3. See the online Help for procedures to upgrade or remove software.

Software Upgrade Notes

Release 4.2 introduced system software licensing. Be sure to review the information in the next topic, System Software Licensing, before you upgrade your system software.

- See the *Software Upgrade Procedure*, which is available on the *NBX Resource Pack DVD* or from www.3com.com, for information about how to upgrade a specific release of software.
- To run system software release R4.2 and higher, you must install a license key.
- A license key is required only for upgrading to major releases, RX.X. All minor releases, RX.X.X, use the corresponding major release license key.
- To upgrade a system to release R4.3 first upgrade to release R4.2.
- To upgrade a system to release R4.2 first upgrade to release R4.1.
- A 4.3 license is valid for both a 4.1-to-4.2 upgrade as well as the 4.2-to-4.3 upgrade.
- When you upgrade the system software, do not enter any "cd..." commands using the terminal emulation software on a PC attached to the Call Processor.

- When the software upgrade is complete, a window that contains a confirmation message displays in the NBX NetSet utility.
- Before you upgrade your system software, 3Com recommends that you back up your system data. (See "System Backup" on page 75.)
- If you are using PC applications, such as the pcXset application, you must also upgrade these applications after upgrading the software.
- If you are using the NBX Call Reports application, install the latest version of the application from the NBX Resource Pack DVD or the NBX Partner Access web site.
- If you are connected to the Call Processor COM1 port, you see the upgrade activity messages during the upgrade process, but you cannot issue any commands.
- After you upgrade your system software, reboot the system.

System Software Licensing

To run release R4.2 and all later releases of the V3000 system software on your system, you must have and install a license. A license key is required only for upgrading to major releases, RX.X. All minor releases, RX.X.X, use the corresponding major release license key. All systems that are shipped from the factory with software release R4.2 or any later release, include a license for the software version that is shipped with the system.

Upgrading to R4.2 From a Previous Release

To upgrade a system to release R4.2 first upgrade to release R4.1.

Upgrading From R4.1.14 and Prior Releases

If your system software is release R4.1.14 or a previous release, you cannot enter the license key for R4.2 before you upgrade because the system software will not recognize the R4.2 license as valid.

Use these steps to upgrade to R4.2:

1. Upgrade to R4.2 in the usual way.
2. Reboot to R4.2.
3. When you see the warning message that indicates you must install a license, click the License button and install the R4.2 license.

If you decide not to install the R4.2 license key, you can click the Reboot button and select a different release.

Upgrading From R4.1.15 and Later Versions

If you are running R4.1.15 or a later release of R4.1, you can enter the R4.2 license key and then upgrade. When you enter the license key, the system software accepts the license key as valid for an unknown feature. When you upgrade and reboot to R4.2, the license for R4.2 takes effect.

Upgrading From Release 4.2

If you are running R4.2 and you upgrade to a new software version, the final step is to reboot the system specifying the new release. At that time, the software verifies that you have the proper license installed. If you have installed the license prior to the reboot, the upgrade is completed.

If you have not installed the correct license prior to the reboot phase of the upgrade, the system provides a warning message and guidance on the appropriate action for you to take.

Restricted Operation

If you reboot the system without installing the required license, the system remains operational with these restrictions:

- the NBX NetSet utility is not available.
- Each telephone display panel periodically displays a NO LICENSE message.
- Auto discovery is turned off for all device types.
- Voice mail messages are not allowed.
- The Automated Attendant software is not operational.
- The ability to configure user groups and Automated Attendants from a telephone is not operational.
- If you use a terminal emulation software application, such as Hyperterm, to connect a PC to the system COM1 port, the system sends a message to the Hyperterm application to indicate that a required software license has not been installed.

If you log on using the administrator ID and password, a window appears giving you two options:

- *You can click the* Reboot *button to go to a reboot window and reboot to a previous software release.*
- *You can click the* License *button to go to a license window and enter a license key for R4.2.*

The installation of a valid upgrade license removes all restrictions without the need for a system reboot operation.

Considerations

Some situations require specific actions because of the system software licensing mechanism.

Chassis or Disk Tray Replacement

If you have an NBX 100 system and you need to replace the main system chassis for any reason, provide a valid license backup file to your 3Com NBX Voice-Authorized Partner. This file enables them to provide you with license keys equivalent to those that were associated with the replaced chassis.

If you have a V5000 system and you need to replace the system disk tray for any reason, provide a valid license backup file to your 3Com NBX Voice-Authorized Partner. This file enables them to provide you with license keys equivalent to those that were associated with the replaced disk tray.

If you have a V3000 system and you need to replace the main system chassis for any reason, provide a valid license backup file to your 3Com NBX Voice-Authorized Partner. This file enables them to provide you with license keys equivalent to those that were associated with the replaced chassis.

Licenses for Future Releases

If you purchase a license for a future software release, all software releases up to that version are included. For example, if you purchase a license for release R6.0 and you are currently running release R5.0, you can upgrade to any release R5.X release without the need to purchase an additional license.

Downgrading to Previous Releases

If you are running R4.2 with a valid system software license and you want to downgrade to a previous, unlicensed software version (for example, R4.0 or R4.1) you can do so by rebooting to the previous version. No other action is required.

Customer Service

If you reboot to R4.2 without installing a valid license, and you run your system with the restrictions in place (see "Restricted Operation" on page 366), 3Com Customer Service cannot access the information

required to help you with problems. To obtain assistance from 3Com Customer Service, either reboot to a previous version of the system software or install a license for R4.2.

Third-Party Drivers

You can add and configure third-party telephones for use on a system. The third-party vendor supplies the interface hardware and a software package to support the telephones.

The process of adding third-party telephones includes these steps:

- **Install the device type license** — Each third-party device type (typically a telephone) must be licensed for use on the system. The license governs the type of device and the number of devices of that type that can be added to the system.
- **Installing the software driver** — This step places the third-party driver software on the system disk.
- **Importing the software driver** — This step activates the third-party driver software.

See the online Help for more information about these procedures.

To remove a third-party driver, you must either purge the system database, or revert to a previous database in which the third-party driver was not installed.

Software Upgrades

When you upgrade the system software, you do not need to reinstall and import the third-party drivers, provided that you continue to use the same system database after the upgrade.

If you upgrade the system software and choose to start with a new database, or if you revert to a database that did not include the third-party driver, import the third-party driver again.

Third-Party Telephone Groups

When you install and import a third-party driver, the system creates a new telephone group for the third-party telephone type. When you add third-party telephones to the system, by default the system adds them to this group.

You cannot delete the default third-party telephone group.

A third-party telephone can belong to the default third-party telephone group, or to a telephone group that you create for that third-party telephone.

15 REPORTS

This chapter describes how to access details of system data traffic. It describes these topics:

- Directory
- Device List
- System Data

For more information about these topics and configuration procedures, see the online Help.

Directory

The system provides a directory listing of all the telephone extensions in the system (except for special use extensions such as TAPI Route Point extensions).

If the Auto Attendant picks up a call, the caller can use the telephone's key pad to type the first letters of a person's last name to search this directory. The Last Name parameter of each user profile forms the dial-by-name directory.

The directory includes only mailboxes that have been initialized and have a recorded greeting. The directory does not include special purpose mailboxes, such as a mailbox associated with a TAPI Route Point. You can exclude a user from the directory when you add or modify a user.

To view, print, or search the system directory, click *Reports* > *Directory* and see the online Help for more information.

Device List

The system provides a list of the devices and functions that are currently being used, such as telephones, line card ports, voice mail ports, Call Park extensions, and Groups.

To view or print a report of system devices, click *Reports* > *Device List* and see the online Help for more information.

System Data

The system provides basic data about the system.

Before you contact your 3Com Voice - Authorized Partner or 3Com Technical Support, access this report and record the information.

To view system data, click *Reports* > *System Data* and see the online Help for more information.

V3001R and V5000 systems support disk mirroring and dual power supplies. If your system is configured with disk mirroring or dual power supplies, the System Data window includes a Disk Status button and a Power Supply Status button.

Disk Status

In addition to viewing basic system data, you can also view data specifically about disk drives. If your system is configured for disk mirroring, you can confirm the status of both disks.

To view disk status, click *Reports* > *System Data* > *Disk Status* and see the online Help for more information.

Power Supply Status

If your system is configured with two power supplies, the Power Supply Status report provides the status of each power supply.

To view power supply status, click *Reports* > *System Data* > *Power Supply Status* and see the online Help for more information.

For each power supply, the report displays these types of information:

Table 66 Power Status Report Information

Field	Purpose
Connected	The connection status for each power supply. **Values**: True or False
Output voltage	The output voltage status. **Values**: Valid or Invalid

16 Network Management

This chapter provides information about the tools that you can use to manage the network:

- SNMP
- Syslog
- Event Logging
- Maintenance Alerts

For more information about these topics and configuration procedures, see the online Help.

SNMP

Simple Network Management Protocol (SNMP) is a transport protocol used for network management on IP networks, including remote fault notification and performance monitoring.

SNMP sends messages, called Protocol Data Units (PDUs), between SNMP managers and SNMP agents. Agents store data about themselves in Management Information Bases (MIBs) and return this data to SNMP managers. System users with special rights can be SNMP users and retrieve this data.

You use the NBX NetSet utility to enable and disable SNMP, configure authorized SNMP managers, configure users, and define security.

SNMP topics include:

- SNMP Managers and Agents
- SNMP Security
- Special Considerations
- MIBs and MIB Objects

Terminology and Acronyms

Make sure you are familiar with the following terminology and acronyms, which are commonly used when discussing SNMP operations.

Table 67 SNMP Terminology and Acronyms

Item	Detail
Authentication	Process of ensuring data origin authenticity, specifically that the identity of the user is genuine. Also incorporates data integrity checks, to ensure data has not been altered or destroyed in an unauthorized manner.
CBC	Cipher-Block-Chaining (a method of encoding data encryptions in a message).
HMAC	Keyed-Hash Message Authentication Code. Provides message authentication through the use of cryptographic hash functions.
Inform	Reliable notification of an SNMPv3 event.
Key	A value that is used to ensure authenticity or privacy, without which it is almost impossible to masquerade or eavesdrop.
MD5	Message Digest type 5 (a type of hashing function).
Notification	SNMPv3 event.
Privacy	The hiding of data from eavesdroppers.
SHA	Secure Hashing Function (a type of hashing function).
Trap	SNMPv1 message notifying the manager of a system event.
USM	User-based Security Model.
VACM	View-based Access Control Model.
MIB	Management Information Base.

SNMP Managers and Agents

An agent using network elements stores network information about itself in a Management Information Base (MIB). MIBs specify the variables that network elements maintain. For example, a variable can contain the data that records when you last booted the system.

SNMP managers are network hosts that use SNMP software to poll the network devices and receive the information stored in them.

- Managers use UDP port **161** by default to send requests to the agent
- Agents use UDP port **162** by default to send replies or messages to the manager.

The manager can request data from the agent, or can set variable values in the agent. Agents can reply to the manager's requests, and can also report events.

SNMP collects information two ways:

- SNMP management stations poll the devices on the network.
- Devices send alerts to SNMP management stations.

SNMP has successive iterations as its operations have become more secure. These iteration, in order of greater security, are SNMPv1, SNMPv2, and SNMPv3. The system supports these three modes.

SNMP Security

The system supports these two security models:

- Community Strings — Pre-SNMPv3 standard compatibility
- User-based Security Model (USM) — SNMPv3

The View-based Access Control Model (VACM) applies to both security models.

3Com recommends that you use SNMPv3 because of its enhanced security features.

- Community Strings
- User-based Security Model (USM)
- View-based Access Control Model (SNMPv1, SNMPv2c and SNMPv3)
- Traps, Notifications, and Informs

Community Strings

Community strings is the method by which SNMPv1 manages its own security.

An SNMP *community* is the group to which devices and management stations running SNMP belong, and that determines where to send information. SNMP identifies a community by means of a *community name*.

It is possible for an SNMP device or agent to belong to more than one SNMP community. The SNMP agent does not respond to requests from management stations that do not belong to one of its communities.

The SNMP default communities include Write (private) and Read (public).

User-based Security Model (USM)

The USM of SNMPv3 provides greater security than pre-SNMPv3 configurations. USM includes the following security features:

- Verifies that each received SNMP message has not been modified during its transmission through the network.
- Verifies the identity of the user on whose behalf a received SNMP message claims to have been generated.
- Detects received SNMP messages, which request or contain management information, whose time of generation was not recent.
- When necessary, protects the contents of each received SNMP message from disclosure.

USM provides three levels of security on a per-user basis:

- No authentication and no privacy (no encryption of data)

  This option is comparable to SNMPv1 and does not provide the additional benefits of SNMPv3.
- Authentication provided by Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) with no encryption of data
- Authentication with encryption of data by Data Encryption Standard (DES)

To set an SNMP user's level of security:

1. Login to the NBX NetSet utility using the administrator login ID and password.
2. Click *Network Management > SNMP Settings.*
3. Click a user name.
4. From the Authentication Protocol drop-down list, select the level of security.
5. Click *Apply.*

View-based Access Control Model (SNMPv1, SNMPv2c and SNMPv3)

The View-based Access Control Model (VACM) determines the access rights of a group that users belong to. You can configure each group to have access to a view of the MIB, so that users belonging to that group

can view *only* that portion of the MIB. These views allow access to all MIB objects according to the existing product access restrictions.

Login usernames are the users' security names in this model.

The system checks the access rights for all requests against those applicable to the user's configured access level, that is, the access group. Two groups are supported:

- *Admin* group — View available to Admin group (the highest level) when connected by authenticated means
- *Monitor* group — View available to all other groups, or available when unauthenticated access is used

By default, you are a member of the *Admin* group and you set the access rights of each user (click *Network Management > SNMP Settings)*.

IF objects are read-only due to context only, the system might return the existing SMIv1 error code no-such-name *instead of the enhanced read-only error status on an attempt to set them.*

Traps, Notifications, and Informs

In addition to receiving requests and sending responses to management applications (managers), agents also can send unsolicited messages to managers when they detect some significant event. An unsolicited message is called a *trap* (SNMPv1) or a *notification* (SNMPv2 and SNMPv3). The NBX SNMP agent supports both traps and notifications in all three versions of SNMP.

An *inform* (confirmed notification) is a trap that the agent sends with a request to the manager to acknowledge the receipt of the trap.

the NBX NetSet utility, where the manager IP address can be configured, enables you to configure the target entries.

Ton configure the manager IP address:

1. Login to the NBX NetSet utility using the administrator login ID and password.
2. Click *Network Management > SNMP Settings*
3. Click the SNMP Managers tab.
4. Click *Add* or the name of an existing manager.

5 Edit the fields appropriately.

6 Click *Apply*.

Enterprise notifications use an snmpTrapOID, which consists of the 3Com enterprise number (43), a zero, and the SNMPv1 trap number.

Special Considerations

Make sure you understand this information as you plan to use SNMP in your network:

- The system does not back up SNMPv3 Engine ID, privacy keys, or authentication.

  If you restore keys, you might need to reinitialize them on both the client and the server before they are usable. However, the system does back up notification targets.
- You must back up SNMP as a part of your general system backup operations.
- The system does not display Authentication and Privacy keys.
- You cannot use the same password for the Authentication and Privacy keys.
- When you enable Syslog, the system logs the results of a SNMPv1, SNMPv2, and SNMPv3 `set` operation. In this case:
  - The SNMPv1 Read community string is logged. (SNMPv1).
  - The Security Name is logged (SNMPv2, SNMPv3).
  - The Set result codes are the enhanced SNMPv2/3 error codes.
  - Updates to the user passwords and keys are not logged.

MIBs and MIB Objects

This section lists the MIBs and MIB objects that the system uses as a part of its standard operations.

- MIBs Used on the System
- Standard SNMPv3 MIBs
- Other IEEE/RFC MIBs
- 3Com MIB Objects
- Diagnostics for 3Com MIB Objects
- Persistent Storage

- Agent Conformance Reference
- Network Management Applications
- Applicable Endpoints

MIBs Used on the System

The system supports these public MIBs as read-only objects:

Table 68 Standard MIBS Supported by the System

RFC	Description	Notes
RFC 1155	Structure and Management Information for TCP/IP Networks	Fully supported.
RFC 1157	SNMP	Fully supported.
RFC 1213	MIB-II	Does not support egp and cmot groups.
RFC 1215	Defining Traps	Does not support the 'warm-start' trap.
RFC 1901	SNMPv2	You cannot do SNMP SET on any of the objects by default using either V1 or V2. Read/Write access is removed for the SNMP V1, V2 versions.
RFC 1907	SNMPv2 MIBs	Fully supported.
RFC 2571	SNMP Management Frameworks	Fully supported.
RFC 2572	SNMP Message Processing and Dispatching	Fully supported.
RFC 2573	SNMP Applications	Fully supported.
RFC 2574	User-based Security Model for SNMPv3	Fully supported.
RFC 2575	View-based Access Control Model (VACM)	Context names are restricted to `monitor` (read only) and `admin` (read/write).
RFC 2576	Co-existence Among SNMPv1, SNMPv2, and SNMPv3	Fully supported.
RFC 2737	Entity MIB	Only the EntPhysicalTable is supported.

Refer to "Standard SNMPv3 MIBs" on page 380 for more information.

The system also uses the 3Com NBX Enterprise MIB (a private MIB) to show gateway and telephone information. To examine the 3Com private MIB, see to "NBX Enterprise MIB" on page 511 in this guide.

Standard SNMPv3 MIBs

The system supports the following standard SNMPv3 MIBs. Where applicable, you can configure SNMPv2 through these MIBs as well.

- *SNMP-FRAMEWORK-MIB*

  Supported: The standard Framework and Conformance MIB

- *SNMP-MPD-MIB*

  Supported: The standard Message Processing and Dispatch MIB and Conformance MIB

- *SNMP-TARGET-MIB* and *SNMP-NOTIFICATION-MIB*

  Supported: The standard Target, Notification, and Conformance MIBs

  Filter-related tables might impose a maximum limit of zero entries, effectively disabling this feature. The system supports up to eight notification targets entries.

- *SNMP-USER-BASED-SM-MIB*

  Supported: The standard User-based Security Model and Conformance MIB

  The default table is initialized according to the Security Posture of minimum-secure. User table entries are instantiated and keys are generated based on each system login user name and password in force when the SNMPv3 software version is first upgraded.

- *SNMP-VIEW-BASED-ACM-MIB*

  Supported: The standard View-based Access Control Module and Conformance MIB

  This MIB is read-only and has permanent entries. The default security configuration is *initial-minimum-security-configuration*.

  The *vacmSecurityToGroupTable* contains the current mapping of usernames to groups. One row exists for each username configured.

  The *vacmAccessTable* contains four permanent entries (one for each access level) and one additional entry for security access.

- *SNMP-COMMUNITY-MIB*

  The standard Community and Conformance MIB is *not* required.

Other IEEE/RFC MIBs

The NBX Enterprise MIB, which is a private MIB, provides information about the status of the system. See Appendix G on page 373 for more information.

3Com MIB Objects

Information relating to the gateways and phones attached to the Call Processor might be defined either as a private MIB or by using the 3Com Enterprise MIB.

Call Processors, Gateways, and Telephones

MIB objects representing the following exist for the Call Processors, gateways, and phones:

- Device serial number Device 3C part number
- Device HW version
- SW version
- Device class (i.e. phone, ATA, TLIM, BRI, T1, PRI, ATC, etc.)
- IP address
- IP mask
- IP gateway
- Physical address
- Description
- Device Name

Network Settings

MIB objects representing the following exist for the Call Processor.

- IP On-The-Fly settings
- QoS settings

Gateways

MIB objects representing the following must be implemented for gateways (Analog Line Cards and Digital Line Cards):

- Chassis in which the card is contained
- Slot number

Digital Line Cards

MIB objects representing the following must be implemented for the Digital Line Cards (T1 / ISDN PRI / ISDN BRI):

- Number of channels on board
- T1 SPAN list configuration:
  - MAC address

        - name ID
        - framing
        - line code
        - line length
        - timing mode
        - number of channels
        - number of channels on-line
        - number of channels off-line
    - ISDN PRI SPAN list configuration
        - MAC address
        - Name
        - Type
        - CO switch protocol
        - framing type
        - line code
        - line length
        - number of channels
        - number of channels on-line
        - number of channels off-line
    - ISDN BRI SPAN list configuration
        - MAC
        - ID
        - CO switch protocol
        - TEI manual/auto
        - TEI ID
        - number of channels
        - number of channels on-line
        - number of channels off-line
    - T1 channel list configuration
        - group name

- channel name
- span id
- channel id
- channel mac
- extension, protocol
- direction
- start type
- incoming digit format
- called party digits
- outgoing digit format
- autoExt

- ISDN channel list configuration
  - group name
  - channel name
  - span id
  - channel id
  - channel mac
  - extension
  - autoExt

Diagnostics for 3Com MIB Objects

Diagnostic and statistical information for the system must be made available through MIB objects that represent the following:

Call Processor

- Number of active calls
- Number of Licenses used
- Number of buffer allocation failures
- Memory utilization
- Disk Usage

Gateways (ALCs, DLCs):

- Number of available ports

Telephones:

- Voice quality metrics

Digital line cards (T1/ISDN PRI/ISDN BRI):

- T1/ISDN Board status:
  - Unknown, Ready, Offline, Online, Red Alarm, Blue Alarm, Yellow Alarm
- T1/ISDN SPAN status:
  - Unknown, Ready, Offline, Online, Red Alarm, Blue Alarm, Yellow Alarm
- ISDN SPAN D channel status
  - Unknown, Up, Down
- T1/ISDN Channel status
  - Unknown, Ready, Offline, Online, Red Alarm, Blue Alarm, Yellow Alarm.
- T1/ISDN Channel error count
- T1/ISDN Channel last error code
- Quality performance metrics (as defined in RFC 2495)

Traps and Informs

The system generates traps and Informs for the following events:

- Call Processor coldstart
- Call Processor Power up/down
- Call Processor out of buffer threshold
- Call Processor IP change
- Fan failure (V5000 systems)
- Power supply failure (V5000 systems)
- Temp Threshold exceeded (V5000 systems)
- Malicious Call tagged
- Emergency (911) call initiated
- Voice mail ports exhausted
- Failed logon attempt for admin or user

- License adds/deletes
- License limits thresholds
- VTL connection failure
- Phone Online/Offline
- Phone IP change
- Gateway Online/Offline
- Gateway IP change
- Gateway all ports busy
- Gateway Link state change
- T1/ISDN Board status change
- T1/ISDN SPAN status change
- ISDN SPAN D channel status change
- T1/ISDN Channel status change

System Reinitiation

The system must execute the following commands as a result of invoking an SNMP `set` operation on the system:

- Set NCP reboot (including a scheduled reboot)
- Set NCP shutdown now
- Set reboot now for each gateway
- Set T1/ISDN channel restart now

NCP refers to the Call Processor.

Persistent Storage

All new MIB objects are stored in the system database except Privacy and authentication passwords.

Agent Conformance Reference

Table 69 shows the release R6.0 support for functions defined in the SNMPv3 Framework (RFC).

Table 69 SNMPv3 Agent Conformance for NBX Systems

SNMPv3 RFC	Recommended	Release R6.0+ Support
General		

Table 69 SNMPv3 Agent Conformance for NBX Systems

SNMPv3 RFC	Recommended	Release R6.0+ Support
SNMPv2c Support	Yes	Yes
SNMPv3 Support	Yes	Yes
Management Framework Architecture	Yes	Yes
Transport Mapping - UDP	Yes	Yes
get-bulk support	Yes	Yes
SMIv1	No	Yes
SMIv2	Yes	Yes
Security		
User-based Security Model	Yes	Yes
HMAC-MD5-96	Yes	Yes
HMAC-SHA-96	Yes	Yes
CBC-DES	Yes	Yes
Community-based Security Model	Yes	Yes
Access Control		
User-defined Groups	Yes	No
User-defined Views	Yes	No
Full support of Read-only Views	Yes	No
Command Responder		
noAuthNoPriv	Yes	Yes
authNoPriv	Yes	Yes
authPriv	Yes	Yes
Notification Originator		
Unconfirmed notifications	Yes	Yes
Confirmed notifications	Yes	Yes
Target filtering	Yes	No
noAuthNoPriv	Yes	Yes
authNoPriv	Yes	Yes
authPriv	Yes	Yes

Table 69 SNMPv3 Agent Conformance for NBX Systems

SNMPv3 RFC	Recommended	Release R6.0+ Support
CLI		
Full management	Yes	No
Web		
Full management	Yes	No
MIBs		
SNMP-FRAMEWORK-MIB	Yes	Yes
SNMP-MPD-MIB	Yes	Yes
SNMP-TARGET-MIB	Yes	Yes
SNMP-NOTIFICATION-MIB	Yes	Yes
SNMP-USER-BASED-SM-MIB	Yes	Yes
SNMP-VIEW-BASED-ACM-MIB	Yes	Yes
SNMP-COMMUNITY-MIB	Yes	No

Network Management Applications

The NBX SNMP agent interoperates with the following SNMPv3 products:

- 3Com EMS (when available)
- MG-Soft MIB browser 9.0 for Windows XP
- HP Openview

Applicable Endpoints

Examine the list of 3Com and third-party products in Table 70 to see which products can have information returned through representative MIB objects.

The system provides some proxy information about telephones.

Table 70 Applicable Endpoints

PRODUCT / DEVICE	Part Number	Feature Supported?
3Com Telephones		
1102A Business Phone	3C10121 or 3C10122	Yes
2102A Bus Phone (Lisbon)	3C10226A or 3C10228IRA	Yes

Table 70 Applicable Endpoints

PRODUCT / DEVICE	Part Number	Feature Supported?
2102B/PE Bus Phone 10/100	3C10226B/PE or 3C10228IRB/PE	Yes
1102B/PE Business Phone 10M	3C10281B/PE	Yes/
2101B/PE Basic Phone	3C10248B/PE	Yes
3100 Entry SL Phone	3C10399A	Yes
3101 Basic Phone	3C10401A	Yes
3101SP Basic Phone	3C10401SPKRA	Yes
3102 Business Phone	3C10402A	Yes
3102B Business Phone	3C10402B	Yes
3103 Manager Phone	3C10403A	Yes
3106C Cordless Phone	3C10406A	Yes
3107C Cordless Phone	3C10407A	Yes
Adjuncts		
1105 Attendant Console	3C10123A or 3C10124	Not Applicable
3105 Attendant Console	3C10405A	Not Applicable
Analog Adapters		
1-port ATA (original -and -INT versions)	3C10120 and 3C10120B-xx	No
1-port ATA (Wednesday 2nd-gen ATA)	3C10400	Yes
4-port ATC (original and intermediate versions)	3C10117 and 3C10117B-INT	No
4-port ATC (2nd-gen)	3C10117C	Yes
Analog Line Cards		
ALC (original TLIM)	3C10114	No
ALC (Australia TLIM)	3C10114-ANZ	No
ALC (2nd-gen)	3C10114C	Yes
Digital Line Cards		
BRI-ST Card	3C10164/A/C-ST	No
T1 Card (orig.)	3C10116/B/C	No
E1 Card (orig.)	3C10165/A/C	No
T1 Card (2nd-gen)	3C10116D	Yes
E1 Card (2nd-gen)	3C10165D	Yes

Table 70 Applicable Endpoints

PRODUCT / DEVICE	Part Number	Feature Supported?
Call Processor Level Devices		
Music On Hold Device	N/A	No
External Paging Device	N/A	No
Voice Mail Server	N/A	No
PC Audio Products		
pcXset application	Software	No
WAV Driver	3C10319 Software	No
ConneXtions	Software	No
3rd-Party Products		
Polycom IP3000 Speakerphone	2200-06632-001	No
Citel - Nortel Gateway-Norstar	1271-3C16N	No
Citel - Nortel Gateway -M1	1486-3C19M1	No
Citel - HDAGC	Not Defined	No

Syslog

The Syslog protocol provides a transport mechanism that allows a device to send event notification messages across an IP network to a Syslog server that acts as an event message collector.

The system uses the standard 3Com logging mechanism to log event messages from devices. Since the content of Syslog messages does vary across the networking industry, the formatting and the contents of the messages also vary.

The Syslog protocol is designed to transport these event messages only. In all cases, there is one device that originates the message. The Syslog process on that machine might send the message to a collector. The collector does not send an acknowledgement of the receipt.

The contents of a message have also been at the discretion of its creator. 3Com recommends that you write the messages so that they are informative to the person who might be reading them. It has also been considered good practice to include a timestamp and some indication of the sending device and the process that originated it in the messages.

■ Transport Mechanism

Transport Mechanism

Syslog uses the User Datagram Protocol (UDP) as its underlying Transport layer mechanism. UDP port **514** is the Syslog port.

3Com recommends that the source port also be 514 to indicate that the message is from the Syslog process of the sender. If the sender uses a source port other than 514, 3Com recommends that subsequent messages are from a single consistent port.

Terminology

Here are some Syslog terms which you must be familiar:

- A machine that can generate a message is called a *device*.
- A machine that can receive the message and forward it to another machine is called a *relay*.
- A machine that receives the message and does not relay it to any other machines is called a *collector*. This has been commonly known as a *Syslog server*.
- Any device or relay is known as the *sender* when it sends a message.
- Any relay or collector is known as the *receiver* when it receives the message.
- Senders send messages to relays or collectors with no knowledge of whether it is a collector or relay.
- Senders might be configured to send the same message to multiple receivers.
- Relays might send all or some of the messages that they receive to a subsequent relay or collector. In the case where they do not forward all of their messages, they are acting as both a collector and a relay. In the following diagram, these devices will be designated as relays.
- Relays might also generate their own messages and send them on to subsequent relays or collectors. In that case, a relay is acting as a device.

3Com Implementation

The IP address of the Syslog server, ports, and the status of the Syslog servers are persistent across reboots.

By default, Syslog starts up at every reboot with only error messages checked in as default and sends the log messages to the enabled Syslog servers. You can implement up to three Syslog servers.

For information about how to configure Syslog, see the online Help.

Syslog Message Components

This section describes how to format Syslog messages for transport.

The full format of a Syslog message has three discrete components:

- PRI (Priority) Message Component
- Header Component
- MSG Component

The total length of the packet must be 1024 bytes or less. There is no minimum length for the Syslog message, although it is a waste of resources to send Syslog packets with no contents. The contents of a message are at the discretion of its creator.

PRI (Priority) Message Component

The PRI portion of a Syslog message must have the following characteristics:

- Three, four, or five characters
- Be bound with angle brackets as the first and last characters.

  The PRI portion starts with a leading less-than (<) character, followed by a number, which is followed by a greater-than (>) character.

  The less-than character is defined as the Augmented Backus-Naur Form (ABNF) %60, and the greater-than character has an ABNF value of %62. The number contained within these angle brackets is known as the Priority value, and represents both the Facility and Severity, as described in the section "Facilities Codes and Severity Message Codes".

  The Priority value consists of one, two, or three decimal integers (ABNF DIGITS) using values of %d48 (for 0) through %d57 (for 9).

Facilities Codes and Severity Message Codes

The Facilities codes and Severity Message codes are numerically coded with decimal values.

Some of the operating system daemons and processes have been assigned Facilities values. Processes and daemons that have not been explicitly assigned a Facility might use any of the *local use* facilities, or they might use the *user-level* Facility.

Those Facilities that have been designated are shown in Table 71 along with their numerical code values.

Table 71 Facility Codes

Code Value	Facility Code
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages ■ Various operating systems have been found to utilize Facilities 4, 10, 13 and 14 for security/authorization, audit, and alert messages which seem to be similar.
5	messages generated internally by Syslog
6	Line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon ■ Various operating systems have been found to utilize both Facilities 9 and 15 for clock (cron/at) messages.
10	security/authorization messages ■ Various operating systems have been found to utilize Facilities 4, 10, 13 and 14 for security/authorization, audit, and alert messages which seem to be similar.
11	FTP daemon
12	NTP subsystem
13	log audit ■ Various operating systems have been found to utilize Facilities 4, 10, 13 and 14 for security/authorization, audit, and alert messages which seem to be similar.
14	log alert ■ Various operating systems have been found to utilize Facilities 4, 10, 13 and 14 for security/authorization, audit, and alert messages which seem to be similar.

Table 71 Facility Codes

Code Value	Facility Code
15	clock daemon ■ Various operating systems have been found to utilize both Facilities 9 and 15 for clock (cron/at) messages.
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

Each message Priority also has a Severity level indicator code (decimal). These codes are described in Table 72 along with their numerical values.

Table 72 Severity Level Codes

Numerical Code	Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

Renamed Facilities

The RFC facilities Local Use 0 through Local Use 3 are renamed as Devices, Applications, CallP, and Interface Layers. Table 73 shows you the system facilities renamed from their RFC counterparts.

Table 73 Renamed Facilities From RFC Facilities

Numerical Code	Renamed Facilities	RFC Facilities
16	Devices	Local use 0

Table 73 Renamed Facilities From RFC Facilities

Numerical Code	Renamed Facilities	RFC Facilities
17	Applications	Local use 1
18	CallP	Local use 2
19	Interface Layers	Local use 3

System Log Handles

Table 71 and Table 72 show you the available facilities and severities. The standard facilities are mapped to system log handles, as shown in Table 74:

Table 74 Facilities Mapped to the System Log Handles

Log Handles	Numerical Code	Facility
__TaskInit__	0	kernel messages
AccountCode	10	security/authorization messages
AIncomingDe...	0	kernel messages
ATA	16	Devices
AutoAttApp	17	Applications
AutoAttApp1	17	Applications
AutoAttApp2	17	Applications
AutoAttApp3	17	Applications
BasicSet	16	Devices
BasicSet12	16	Devices
Bitmail	2	mail system
BRIChannel	16	Devices
Call	18	CallP
CallControl	18	CallP
CallGroup	18	CallP
CDR	17	Applications
COFlash	18	CallP
ConfDrop	18	CallP
Conference	18	CallP
ConfPool	18	CallP
COSOverride	18	CallP
DBI	19	Interface Layers(DBI,DIL)

Table 74 Facilities Mapped to the System Log Handles

Log Handles	Numerical Code	Facility
DelayedAnn	18	CallP
DevManager	16	Devices
DiagCLI	18	CallP
DIL	19	Interface Layers(DBI,DIL)
Disks	0	kernel messages
Dnld	17	Applications
DssBlf	16	Devices
Elvis	16	Devices
ExternalVM	17	Applications
Factory	18	CallP
FeatureConfig	18	CallP
Forward	18	CallP
H3LinkLayer	3	system daemons
HuntGroup	16	Devices
HuntGroupLo...	16	Devices
i18n	17	Applications
IMAP	2	mail system
IntVM	2	mail system
IntVM6	2	mail system
IntVM64	2	mail system
IntVM642	2	mail system
IntVM643	2	mail system
IPPool	3	system daemons
LastNumDial	18	CallP
License	4	security/authorization
messages(note1)		
LockUnlock	4	Security/Authorization(note1)
MailStatSrvr	2	mail system
MediaServer	17	Applications
MWB1	18	CallP
MWB2	18	CallP
MWIToPhone	18	CallP
NBSetBus	16	Devices

Table 74 Facilities Mapped to the System Log Handles

Log Handles	Numerical Code	Facility
NBSetBus11	16	Devices
NBSetBus13	16	Devices
nbxINetNot	3	system daemons
nbxNotMgr	3	system daemons
Notifier	3	system daemons
Notifier1	3	system daemons
Notifier5	3	system daemons
Notifier6	3	system daemons
Notifier7	3	system daemons
OrigSession	18	CallP
OrigStartup	18	CallP
OutDialT	17	Applications
OutDialT1	17	Applications
OutDialT2	17	Applications
OutDialT3	17	Applications
PageGroup	18	CallP
ParkZone	18	CallP
Performance	0	kernel messages
PickupClient	3	system daemons
PickupServer	3	system daemons
PRIChannel	16	Devices
RDC	16	Devices
Remote	16	Devices
RoutePoint	18	CallP
Router	0	kernel messages
Server	0	kernel messages
ServManager	0	kernel messages
Span	0	kernel messages
SpeedDial	18	CallP
SystemInfo	0	kernel messages
T1Board	16	Devices
T1Channel	16	Devices
TelephonyDNS	3	system daemons

Table 74 Facilities Mapped to the System Log Handles

Log Handles	Numerical Code	Facility
TermSession	18	CallP
TermStartup	18	CallP
Tlim	16	Devices
Transfer	18	CallP
UserPassword	4	security/authorization messages
VAILSess	17	Applications
VAILSess1	17	Applications
VAILSess2	17	Applications
VAILSess3	17	Applications
VAILSess4	17	Applications
VAILSess5	17	Applications
VAILSess6	17	Applications
VAILSess7	17	Applications
VAILSess8	17	Applications
VApplL	17	Applications
VoiceApp	17	Applications
VoiceApp1	17	Applications
VoiceApp2	17	Applications
VoiceApp3	17	Applications
VoiceApp4	17	Applications
VoiceApp5	17	Applications
VoiceApp6	17	Applications
VoiceApp7	17	Applications
VoiceApp8	17	Applications
VoiceMail	17	Applications
VoiceMail1	17	Applications
VoiceMail2	17	Applications
VoiceMail3	17	Applications
VTL	18	CallP
VTLMerge	18	CallP
WEB	3	system daemons
YAVA	17	Applications
DBR	19	Interface Layers(DBI,DIL)

Table 74 Facilities Mapped to the System Log Handles

Log Handles	Numerical Code	Facility
Adminlog	13	log audit(note1)
SNMP traps	14	log alert(note1)

The current administration log messages are classified to only one facility; that is, log.

The Priority value is calculated as follows:

1 Multiplying the Facility number by the number eight

2 Adding the numerical value of the Severity

Examples:

- A kernel message (Facility=0) with a Severity of Emergency (Severity=0) has a Priority value of zero (0).
- A `local use 4` message (Facility=20) with a Severity of Notice (Severity=5) has a Priority value of 165.

  In the PRI part of a Syslog message, these values would be placed between the angle brackets as <0> and <165, respectively. The only time a value of zero follows the less-than character is when the Priority value is zero. Otherwise, leading zeroes must not be used.

Header Component

The Header component of the Syslog message must contain the following:

- A timestamp
- An indication of the hostname or IP address of the device
- Visible (printing) characters
- A seven-bit ASCII code set in an eight-bit field like that used in the PRI part.

  In this code set, the only allowable characters are the ABNF VCHAR values (%d33-126) and spaces (SP value %d32).

The Header contains two fields called the TIMESTAMP and the HOSTNAME.

TIMESTAMP Field

The TIMESTAMP field contains the local time. The TIMESTAMP field immediately follows the trailing > character of the PRI portion of the Syslog packet.

Field Format The format of the TIMESTAMP field is:

```
Mmm: dd: hh:mm:ss
```

where the format is interpreted as follows:

Table 75 TIMESTAMP Field Format

Value	Description
`Mmm`	The English language abbreviation for the month of the year, with the first character in uppercase and the other two characters in lowercase. The following are the only acceptable values: ■ Jan ■ Feb ■ Mar ■ Apr ■ May ■ Jun ■ Jul ■ Aug ■ Sep ■ Oct ■ Nov ■ Dec
`dd`	Day of the month. If the day of the month is less than ten, a space character must precede the month digit. For example, the 7th day of August would be represented as “Aug 7", with two spaces between the “g” and the “7”.

Table 75 TIMESTAMP Field Format

Value	Description
`hh:mm:ss`	The local time. `hh` — Hours represented in 24-hour format. Valid entries are between 00 and 23, inclusive. `mm` — Minutes represented by entries that are between 00 and 59, inclusive. `ss` — Seconds represented by entries that are between 00 and 59, inclusive.

A single space character must follow the TIMESTAMP field.

HOSTNAME Field

The HOSTNAME field contains the hostname.

- If the field does not have a hostname, then it contains the device IP address.
- If a device has multiple IP addresses, common practice is to use the IP address from which the message is transmitted.

An alternate method is to configure a device to send all messages using a single source IP address, regardless of the interface from which the message is sent. This provides a single consistent hostname for all messages sent from a device.

The HOSTNAME field contains only the hostname, the IPv4 address, or the IPv6 address of the originator of the message. The preferred value is the hostname.

A single space character must follow the TIMESTAMP field.

Restrictions Following are the limitations in populating the HOSTNAME field.

- The hostname cannot contain any embedded spaces.
- The domain name must not be included in the HOSTNAME field.
- If the IPv4 address is used, it must be shown as the dotted decimal notation.
- If an IPv6 address is used, any valid representation used in RFC 2373 may be used.
- A single space character must follow the HOSTNAME field.

MSG Component

The MSG component of the Syslog message usually contains some additional information about the process that generated the message, and then the text of the message itself.

There is no ending delimiter to the MSG component.

The MSG component must contain visible (printing) characters. The code set traditionally and most often used has also been seven-bit ASCII in an eight-bit field like that used in the PRI and HEADER parts. In this code set, the only allowable characters are the ABNF VCHAR values (%d33-126) and spaces (SP value %d32).

However, no indication of the code set used within the MSG is required, nor is it expected. Other code sets may be used as long as the characters used in the MSG are exclusively visible characters and spaces similar to those described above.

Select a code set with the intended receiver in mind. A message containing characters in a code set that cannot be viewed or understood by a recipient yields no information of value to an operator or administrator reviewing it.

MSG Component Fields

The MSG component has two fields:

TAG Field — The TAG is a string of ABNF alphanumeric characters that must not exceed 32 characters. Any non-alphanumeric character terminates the TAG field and is assumed to be the starting character of the CONTENT field. The value in the TAG field is the name of the program or process that generated the message.

CONTENT Field — The CONTENT contains the details of the message. This has traditionally been a freeform message that gives some detailed information of the event. Most commonly, the first character of the CONTENT field that signifies the conclusion of the TAG field is the left square bracket character ([ ), a colon character (:), or a space character.

See "Originating Process Information in MSG" for more details.

Domain Name and Address in MSG

To identify the device that originated the message, you might wish to include its Fully-Qualified Domain Name (FQDN) and its IP address within

the CONTENT field. Traditionally, however, only the hostname has been included in the HOSTNAME field.

Originating Process Information in MSG

You might want to include some information about the process on the device that generated the message. This information usually consists of the process name and process ID (often known as the `pid`) for robust applications. The process name is commonly displayed in the TAG field.

Quite often, additional information is included at the beginning of the CONTENT field. The format

```
TAG [PID]:
```

is common. The left square bracket is used to terminate the TAG field in this case, and is then the first character in the CONTENT field. If the process ID is not needed, it may be omitted.

In that case, a colon and a space character usually follow the TAG. This would be displayed as `TAG:`. In that case, the colon is the first character in the CONTENT field.

Syslog Security Considerations

The Syslog process places Event Notification messages into files on that system. This process relies upon the integrity of the system for the protection of the messages. Be aware that event messages might be sent accidentally, erroneously, and even maliciously. Since Syslog is a relatively simple protocol, its operations are not secure to the point where its integrity is robust.

Message Forgery

An attacker might transmit Syslog messages (either from the machine from which the messages are purportedly sent or from any other machine) to a collector. In one case, an attacker might hide the true nature of an attack amidst many other messages.

As an example, an attacker might start generating forged messages indicating a problem on some machine. This might get the attention of the system administrators who spend time investigating the alleged problem. During this time, the attacker might be able to compromise a different machine, or a different process on the same machine.

Additionally, an attacker might generate false Syslog messages to give misleading indications of status or of events. For example, an attacker might stop a critical process on a machine, which might generate a notification of exit. The attacker might subsequently generate a forged notification that the process had been restarted. System administrators might accept that misinformation and not verify that the process had indeed been restarted.

In some cases, to avoid such message forgeries, you can disable the Syslog port on the system when Syslog logging is disabled.

Caution: *Syslog messages sent to the remote server do not employ encryption standards.*

Periodic Timestamp on Console (PTOC)

The PTOC feature sends a timestamp to the system console at a set interval. If the system experiences a problem of any kind, this timestamp can help you identify when the problem occurred. If the time interval is set to *X* minutes, it will print every *X* minutes, whether or not any other messages are printing.

To configure the PTOC:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *Network Management* > *Syslog Settings*.
3. Select a time value from the *Periodic Timestamp on Console* drop-down list.
4. Click *Apply*.

Event Logging

You can view these event logs that the system maintains:

- **Adminlog** — Tracks activities performed in the NBX NetSet utility under the administrator login. The system never renames or deletes the Adminlog. It continues to grow over time, but it is unlikely that the size of the Adminlog file will ever grow to be a problem.

  The system updates the adminlog file whenever system events occur, such as:

  - When you enable or disable Supervisory Monitoring system-wide.
  - When you add, modify, or delete a domain.

- When someone uses the wrong password when attempting to view domain reports in the NBX NetSet utility.
- When a user attempts to monitor another user by activating feature code **425**, and then uses the wrong password. (The log updates after the maximum password retries are exceeded.)

- **Upglog** — Tracks the history of upgrades and processes that occur during upgrades.
- **TEP Logs** — The 3C10116D T1 Digital Line Card and the 3C10165D E1 Digital Line Card can generate logging information. TEP (**T**1, **E**1, **P**rimary Rate Interface) logs are stored on the system disk drive, even for cards that are in remote locations, and you can use the NBX NetSet utility to view, download, and delete log files. Each card has a separate log, up to a maximum of five log files. When a log reaches its maximum size, it begins to overwrite the oldest data.

Because TEP logging has a performance cost, it is disabled by default. To enable TEP logging, contact your 3Com NBX Voice-Authorized Partner.

To view event logs, click *Network Management* > *Event Logging* and see the online Help for more information.

Maintenance Alerts

If you have a V5000 system with disk mirroring or dual power supplies and with NBX Messaging enabled, you can:

- Configure maintenance alert voice mail messages so that they appear to come from one system user.
- Designate up to 15 system users to receive maintenance alerts.

Alert messages are defined by the system. The content depends on the cause of the alert.

When a user receives a maintenance alert message, the source of the message depends on whether you have configured a system user as the author of maintenance alert messages. See Table 76 for details.

Table 76 Source of Maintenance Alert Messages

Message Type	Author Configured	No Author Configured
Local Voice Mail Message	The configured system user is announced as the sender of the message.	An *outside caller* is announced as the sender of the message.

Table 76 Source of Maintenance Alert Messages (continued)

Message Type	Author Configured	No Author Configured
Off-site E-mail Message	The name of the configured system user appears in the *From* field of the e-mail.	The From field in the e-mail contains the word *anonymous*.
Off-site Voice Mail Message	The system user is announced as the sender of the message.	An *outside caller* is announced as the sender of the message.

To set maintenance alerts:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *Network Management* > *Maintenance Alerts*. See the online Help for procedures to set the maintenance alert author and specify users to receive maintenance alerts.

17 COUNTRY SETTINGS

This chapter describes how to manage language settings for your system. It describes:

- Regional Software
- Regional Settings

For more information about these topics and configuration procedures, see the online Help.

Regional Software

Regional software includes local language voice prompts, regional tones and cadences, and local language versions of certain user documentation for your region.

A region is a country and language pair, for example, "China - Mandarin" or "France - French." The system uses English as the default. You must install Country Packs to enable the system to support other languages.

Table 77

Country Pack	Documentation	Prompts	Tones and Cadences
Argentina_es.taz	Latin Spanish	Latin Spanish	Argentina
Australia.taz	US English	Australian English	Australia
Brazil.taz	Brazilian Portuguese	Brazilian Portuguese	Brazil
China.taz	Chinese Traditional (Mandarin)	Chinese Traditional (Mandarin)	China
ChinaHongKong.taz	Chinese Simplified (Cantonese)	Chinese Simplified (Cantonese)	China

Table 77

Country Pack	Documentation	Prompts	Tones and Cadences
NOTE: The LabelMaker utility included as part of the Chinese Country Packs is in US English. PDF-format Chinese LabelMakers are available on the NBX Resource Pack DVD.			
Egypt_en.taz	US English	UK English	Egypt
France.taz	Parisian French	Parisian French	France
Germany.taz	German	German	Germany
Israel.taz	US English	Hebrew	Israel
Italy.taz	Italian	Italian	Italy
Mexico.taz	Latin Spanish	Latin Spanish	Mexico
NewZealand.taz	US English	New Zealand English	New Zealand
Russia.taz	US English	Russian	Russia
SaudiArabia_en.taz	US English	UK English	Saudi Arabia
Spain.taz	European Spanish	European Spanish	Spain
UAE_en.taz	US English	UK English	United Arab Emirates
UnitedKingdom.taz	US English	UK English	United Kingdom

Release R6.0 software includes a localized NetSet utility interface for telephone users (Latin Spanish, Brazilian Portuguese, and Italian). The localized NetSet interface is set by the host computer's browser language setting.

Install Regional Software

To add regional software:

1. Click *Country Settings* > *Install Regional Software*.
2. See the online Help and the notes in the next sections for information about how to manage regional software.

   After you install regional software, you must designate it to be the current system regional software. Click *Country Settings* > *Regional Settings.*

Remove Regional Software

To remove regional software:

1. Click *Country Settings* > *Install Regional Software*.
2. See the online Help and the notes in the next sections for information about how to manage regional software.

   You can remove regional software at any time. The system removes all versions of the regional software that you select. For example, if you choose to remove the "Mexico - Spanish" regional pack, the system removes *all* versions of the selected regional software.

You cannot remove U.S. English.

When you remove a version of system software, the system verifies whether the removal might leave any regional software unassigned to a system software version.

Specific regional languages, tones and cadences, or voice prompts that were associated with earlier releases might no longer be usable by recent system software versions. 3Com recommends that you purge unused regional software to conserve disk space.

You can only remove unused regional software immediately after you delete a version of system software. If you choose not to remove this software when prompted, you must either:

- *Wait until you remove a subsequent version of system software before you can delete any unused regional software.*
- *Remove all versions of the selected regional software on the system. You can then install the required version.*

Regional Details

The Regional Software Diagnostic Details window displays the status of each region in the current system software. Table 78 defines the displayed values.

Table 78 Diagnostic Details

Values	Description
In Use	The regional software is currently being used by the system.
Available	The regional software is fully loaded on the system, but it is not currently in use.

Table 78 Diagnostic Details (continued)

Values	Description
Not Fully Installed	The system can access some parts of the regional software, but not all. You might not have loaded the correct regional software version for the system software you are running.
Error While Loading	An error occurred while loading the regional software. Re-install the software.
Nothing Installed	The system is aware that this regional software exists, but no version is installed.

Regional Settings

After you install regional software and components from the regional packs, you can enable regional settings. To enable these regional settings in NetSet, you select the appropriate country and language for the system voice prompts, the technical tones and cadences, and the online user documentation.

To enable regional settings, select *Country Settings* > *Regional Settings*. See the online Help for the procedure to enable regional settings.

See "Third-Party Drivers" on page 368 for information about how to install regional language packs.

Advanced Regional Settings

The system also allows you to choose different regional settings for the system voice prompts, the technical tones and cadences, and the online user (not administrator) documentation. For example, you might require local tones and cadences but want the documentation to be in English and the voice prompts in Australian English.

You can select separate regional settings for:

- Voice prompts — The Auto Attendant voice prompts.
- Documentation — The *NBX Telephone Guide*, the NBX NetSet user Help, the LabelMaker utility, and the quick reference cards.
- Tones and Cadences — The tones and the patterns of rings (cadence) versus silence. Tones and cadences vary from country to country. Examples:
  - United States ringing cadence (pattern) is 2 seconds of ring followed by 4 seconds of silence.

- United Kingdom ringing cadence is 2 rings within approximately 2 seconds followed by 2 seconds of silence.
- United States busy tone is 0.75 seconds of tone followed by 0.75 seconds of silence.

To enable different regional settings:

1. Log on to the NBX NetSet utility using the administrator login ID and password.
2. Click *Country Settings* > *Regional Settings* > *Advanced Regional Settings.*
3. See the online Help for more information.

18 TROUBLESHOOTING

This chapter contains maintenance and troubleshooting information to help you resolve simple problems. It describes these topics:

The system hardware needs no routine maintenance. However, perform periodic backups of the configuration and license databases, especially after you make changes to system or user configurations.

Using the Telephone Local User Interface Utility

Each 3Com telephone supports a telephone diagnostic and configuration utility called the Local User Interface (LUI). The LUI utility enables you to perform these tasks:

- View telephone settings, both the active settings and the settings stored in the telephone's memory
- Set telephone IP address, subnet mask, and default gateway
- Specify the IP address of the Call Processor
- Test the telephone buttons, display panel, and status lights
- Clear all device settings
- Specify the MAC address of the Call Processor (test environment option)
- View firmware information (technician option)

- Test connectivity
- Restart the telephone

Early model 3Com Telephones support an earlier version of the LUI utility that has a slightly different menu. For information about this earlier version of the LUI utility, see your NBX Voice-Authorized Partner or a version of the NBX Administrator's Guide *from a release prior to release R4.3.*

To start the LUI utility:

1 Cycle power to the telephone by disconnecting and then reconnecting its power connector, and then access the LUI menu options (see step 2) before the telephone finishes its download of code from the Call Processor).

For telephones that use a powered Ethernet cable instead of a power adapter, disconnect and then reconnect the Ethernet cable.

You do not need to cycle power to 3101B and 3102B Business Telephones.

2 To access (or exit from) the LUI utility:

- On the 3Com 3102 and 3102B Business Telephone, press the *Program* button:

- On 3Com1102, 2102, or 2102-IR Business Telephones, press *Program*:

- On 3Com3103 Manager's Telephones and 3101, 3101B, or 3101SP Basic Telephones, press the center button in the cursor control button group:

- On the 3Com 2101 Basic Telephone, press the MSG button:

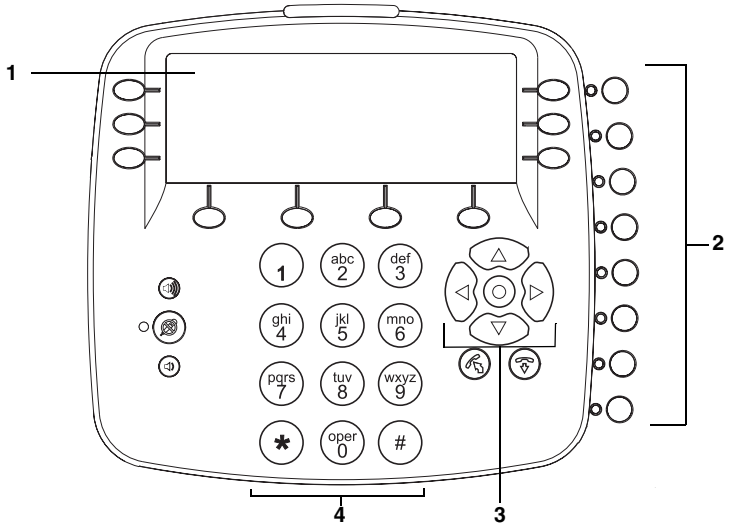
- On 3106C and 3107C Cordless Telephones, press the Feature button:

The buttons you use to enter information vary with each telephone:

- 3Com 3103 Manager's Telephone, see on Figure 27.
- 3Com 3102 and 3102B Business Telephone, see Figure 28 on page 417.
- 3Com 3101, 3101B or 3101SP Basic Telephones, see Figure 29 on page 418.
- 3Com 1102, 2102, or 2102-IR Business Telephones, see Figure 30 on page 419.
- 3Com 2101Basic Telephone, see Figure 31 on page 420.
- 3Com 3106C Cordless Telephone, see Figure 32 on page 421.
- 3Com 3107C Cordless Telephone, see Figure 33 on page 422.

Table 79 on page 423 describes each LUI utility menu item.

Figure 27 Local User Interface Controls on the 3Com 3103 Manager's Telephone



1 Display panel.

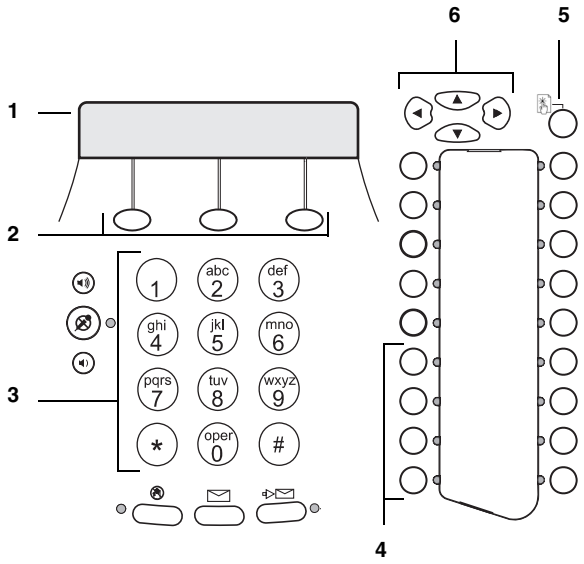
2 Access buttons AB1-AB8 (from bottom to top) select menu items.

3 Scroll buttons:

- Center select button starts and exits from the LUI utility or exits from a menu item and moves to the next higher menu. If you press the center select button before you save a change to a setting, you exit the menu item without saving the change.
- Up and down buttons move up or down through the LUI menu and select hex digits when editing a MAC address.
- Left and right buttons position the cursor in the display panel when you edit a setting, such as an IP address or an Call Processor MAC address.

4 Key pad numeric keys select menu items or enter numeric characters in a menu item. Use the # key to save changes after you edit an item.

Figure 28 Local User Interface Controls on the 3Com 3102 and 3102B Business Telephone



1 Display panel.

2 On 3102 Business Telephones, the soft buttons move the cursor left or right and the middle button is inactive. On 3102B Business Telephones, the soft buttons are inactive.

3 Key pad numeric keys select menu items or enter numeric characters in a menu item. Use the # key to save changes after you edit an item.

4 Access buttons AB1-AB4 (from bottom to top) select menu items.

5 Program button:

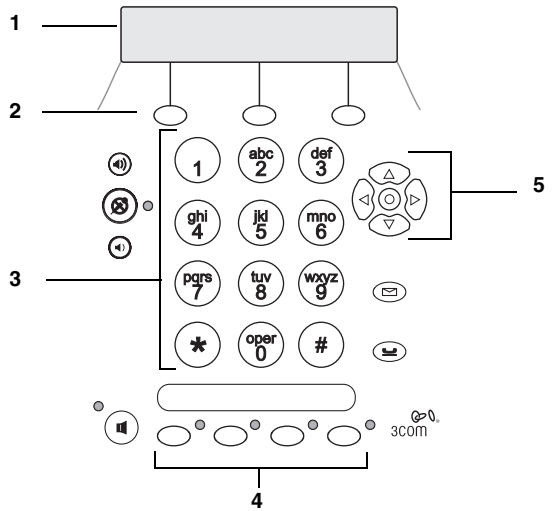
- Start and exit from the LUI utility.
- Exit from a menu item and move to the next higher menu. If you press the Program button before you save a change to a setting, you exit the menu item without saving the change.

6 Scroll buttons:

- Up and down buttons move up or down through the LUI menu and select hex digits when editing a MAC address.
- Left and right buttons position the cursor in the display panel when you edit a setting, such as an IP address. On 3102B Business

Telephones, the left button erases the characters of a setting and the right button is inactive.

Figure 29 Local User Interface Controls on 3Com 3101, 3101B, and 3101SP Basic Telephones



1 Display panel.

2 On 3101 and 3101SP Business Telephones, the soft buttons move the cursor left or right and the middle button is inactive. On 3101B Business Telephones, the soft buttons are inactive.

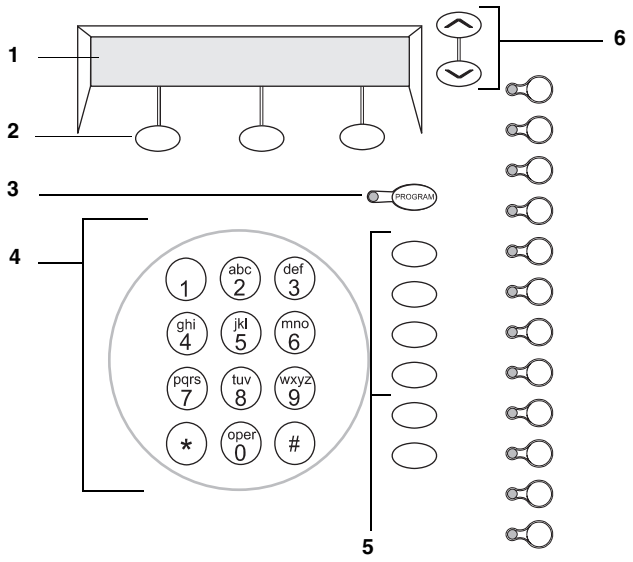
3 Key pad numeric keys select menu items or enter numeric characters in a menu item. Use the # key to save changes after you edit an item.

4 Access buttons AB1-AB4 (from left to right) select LUI menu items.

5 Scroll buttons:

- Center select button starts and exits from the LUI utility or exits from a menu item and moves to the next higher menu. If you press the center select button before you save a change to a setting, you exit the menu item without saving the change.
- Up and down buttons move up or down through the LUI menu and select hex digits when editing a MAC address.
- Left and right buttons position the cursor in the display panel when you edit a setting, such as an IP address. On 3101B Business Telephones, the left button erases the characters of a setting and the right button is inactive.

Figure 30 Local User Interface Controls on the 3Com 1102, 2102,and 2102-IR Business Telephones



1 Display panel.

2 Soft buttons move the cursor left or right. The middle button is not used.

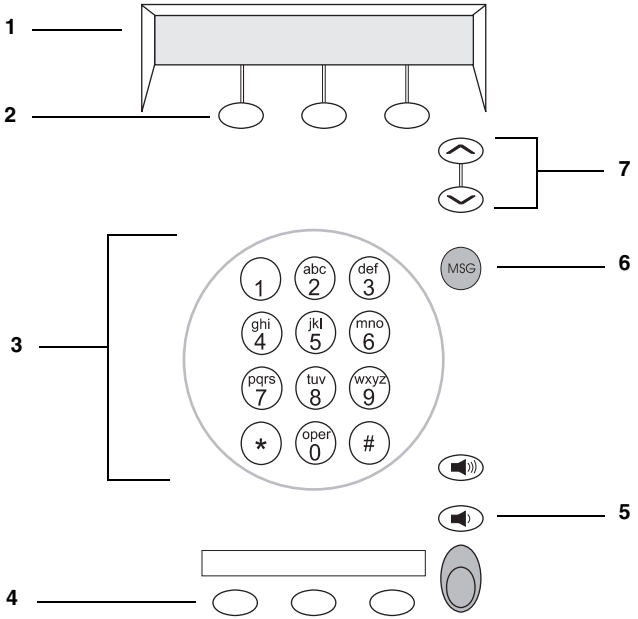
3 Program button starts and exits from the LUI utility or exits from a menu item and moves to the next higher menu. If you press the Program button before you save a change to a setting, you exit the menu item without saving the change.

4 Key pad numeric keys select menu items or enter numeric characters in a menu item. Use the # key to save changes after you edit an item.

5 Access buttons AB1-AB4 (from top to bottom) select LUI menu items.

6 Scroll buttons move up or down through the LUI menu and select hex digits when editing a MAC address.

Figure 31 Local User Interface Controls on the 3Com 2101 Basic Telephone



1 Display panel.

2 Soft buttons move the cursor left or right. The middle button is not used.

3 Key pad numeric keys select menu items or enter numeric characters in a menu item. Use the # key to save changes after you edit an item.

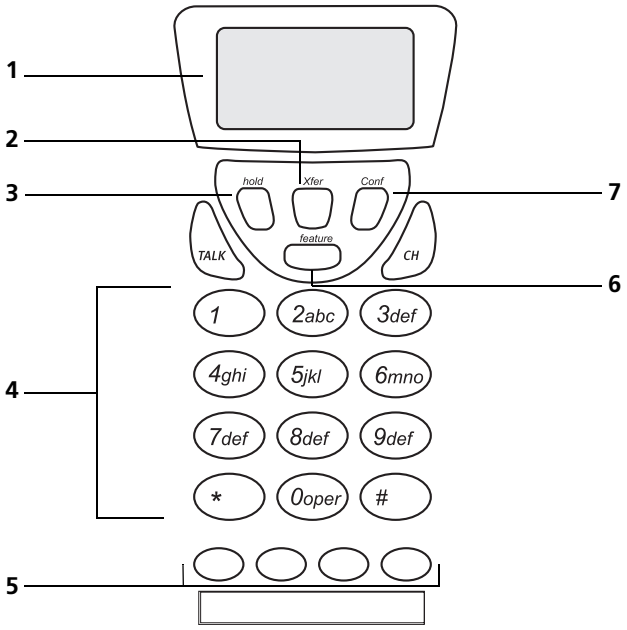
4 Access buttons AB1-AB3 select LUI menu items.

5 Volume Down button selects LUI menu item AB4.

6 MSG (voice mail message) button starts and exits from the LUI utility or exits from a menu item and moves to the next higher menu. If you press the MSG button before you save a change to a setting, you exit the menu item without saving the change.

7 Scroll buttons move up or down through the LUI menu and select hex digits when editing a MAC address.

Figure 32 Local User Interface Controls on the 3106C Cordless Telephone



1 Display panel.

2 Xfer (transfer) button scrolls right in the display panel.

3 Hold button scrolls left in the display panel.

4 Key pad for selecting menu items or entering numeric characters. Use # to commit changes. Use * to exit from a menu item or from the LUI utility. If you have not already saved changes by pressing #, pressing * exits that menu item without saving changes.

5 Access buttons AB1-AB4 (from left to right) select LUI menu items.

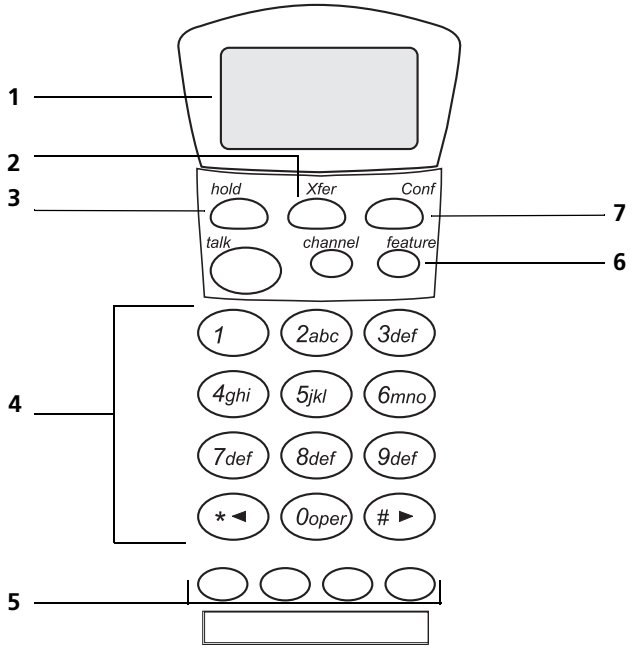
6 Feature button starts the LUI utility. After you start the LUI utility, the Feature button:

- Scrolls up the LUI menu.
- Selects hex digits when editing a MAC address.

7 Conf (conference) button:

- Scrolls down the LUI menu.
- Selects hex digits when editing a MAC address.

Figure 33 Local User Interface Controls on the 3107C Cordless Telephone



1 Display panel.

2 Xfer (transfer) button scrolls right in the display panel.

3 Hold button scrolls left in the display panel.

4 Key pad for selecting menu items or entering numeric characters. Use # to commit changes. Use * to exit from a menu item or from the LUI utility. If you have not already saved changes by pressing #, pressing * exits that menu item without saving changes.

5 Access buttons AB1-AB4 (from left to right) select LUI menu items.

6 Feature button starts the LUI utility. After you start the LUI utility, the Feature button:

- Scrolls up the LUI menu.
- Selects hex digits when editing a MAC address.

7 Conf (conference) button:

- Scrolls down the LUI menu.
- Selects hex digits when editing a MAC address.

Table 79 LUI Menu Items

Menu Option	Description
NOTE: NCP refers to the Call Processor.	
1 View Settings	Press 1 on the number pad and scroll to view these options: **MAC Address** (**My MAC Address** on 3101B and 3102B Business Telephones) – MAC address of this telephone. **NCP MAC Address** – MAC address of Call Processor. All Fs, the normal value for this setting, indicates that the telephone responds to any Call Processor. **SW Build Ident.** – Software version running on this telephone (except on 3101B and 3102B Business Telephones). ***On 3101B and 3102B Business Telephones:*** ■ **SW Build OPs Id** — The current version of the application code on the telephone ■ **SW Build LIB Id** —The current version of the library code on the telephone (used for VCX). ■ **SW Build DSP Id** — The current version of Digital Signal Processor (DSP) code on the telephone. **Serial # Rev** (**Serial Number** on 3101B and 3102B Business Telephones) – Telephone serial number and hardware version. **Phone Port Speed** – Speed and duplex setting of the LAN connection. **PC Port Speed** – The speed and duplex setting of the PC port to the device, if any, connected to the port. **Note:** The next four settings are all valid only if the device downloads via IP (layer 3). These four settings are acquired from either DHCP or a setting in the telephone's memory **My IP Address** – Active IP address of this telephone. **Subnet Mask** – Active IP mask. **Gatwy IP Address** (**Gateway IP Address** on 3101B and 3102B Business Telephones) – Active default gateway IP address. **NCP IP Address** – Active IP address of the Call Processor with which this telephone communicates. **ALT SrvrIP** (**Alt. Server IP** on 3101B and 3102B Business Telephones) – Active IP address of a secondary download server with which this telephone communicates, acquired from either DHCP option 184 or a setting in the telephone's memory. (Valid for 3Com VCX Telephone systems only.)

Table 79 LUI Menu Items (continued)

Menu Option	Description
	VLAN Config (**VLAN Configuration** on 3101B and 3102B Business Telephones) – Active VLAN for this telephone, acquired from either DHCP option 184 or a setting in the telephone's memory. Valid for 3Com VCX Telephone systems only. **Mem- My IP Addr** (except on 3101B and 3102B Business Telephones) – The IP address configured in the telephone's memory though the LUI utility. **Mem- Subnet Mask** (except on 3101B and 3102B Business Telephones) – The IP mask configured in the telephone's memory though the LUI utility. **Mem- Gatwy IP** (except on 3101B and 3102B Business Telephones) – The default gateway IP address configured in the telephone's memory though the LUI utility. **Mem- NCP IP Addr** (except on 3101B and 3102B Business Telephones) – The Call Processor IP address configured in the telephone's memory though the LUI utility. **Mem- ALT SrvrIP** (except on 3101B and 3102B Business Telephones) – Secondary download server address configured in the telephone's memory. (Valid for 3Com VCX Telephone systems only.) **Mem- VLAN Config** (except on 3101B and 3102B Business Telephones) – VLAN values configured in the telephone's memory. Valid for 3Com VCX Telephone systems only. ***For the 3101B and 3102B Business Telephones only:*** ■ **EE-My IP** — The IP address configured in the telephone's memory. ■ **EE-Subnet Mask** — The IP mask configured in the telephone's memory. ■ **EE-Gateway IP** — The default gateway IP address configured in the telephone's memory. ■ **EE-NCP IP** —The Call Processor IP address configured in the telephone's memory. ■ **EE-Alt Server IP** — Secondary download server address configured in the telephone's memory ■ **EE-VLAN Config** — VLAN values configured ■ **Flash - BootStrap** —The version number of the software that starts when telephone first powers up. ■ **Flash Download** —The version number of the software that downloads new code to the telephone. ■ **Flash Operation** — The version number of the operational image on the telephone.

Table 79 LUI Menu Items (continued)

Menu Option	Description
2 Set my IP 3 Set SubNMsk 4 Set Gatwy IP	**Note**: On 3101B and 3102B Business Telephones: 2 Configure IP Address 3 Configure SubNetMask 4 Configure Gateway IP Address Lets you specify the IP information for this telephone. When entering an IP address: ■ Use the key pad to enter digits 0–9. ■ Use the left and right soft keys or scroll keys to move the cursor left or right. ■ If any of the fields within the IP address contain only one or two digits, add leading zeros. Example: Enter 10.234.1.125 as 010.234.001.125 ■ To change a telephone back to its default setting, enter 255 for each octet of the IP address. To clear all configured settings and return to factory defaults, select menu item AB4. **Note**: On 3101B and 3102B Business Telephones, see menu option **6 Advanced Settings > 3 Set EEPROM - Default** for information about how to return 3101B and 3102B Business Telephones to their default settings. ■ Press the # key to commit your address change.
5 Set NCP IP	**Note**: On 3101B and 3102B Business Telephones: 5 Configure NCP IP Address Lets you specify the IP address of the Call Processor. If the telephone is on the same subnet as the Call Processor you never need to specify the Call Processor IP address. If the telephone is on a different subnet, then you must enter this information or provide it by using DHCP option 184. When entering an IP address: ■ Use the key pad to enter digits 0–9. ■ Use the left and right soft keys or scroll keys to move the cursor left or right. ■ If any of the fields within the IP address contain only one or two digits, add leading zeros. Example: Enter 10.234.1.125 as 010.234.001.125 ■ To change a telephone back to its default setting, enter 255 for each octet of the IP address. To clear all configured settings and return to factory defaults, select menu item AB4. ■ Press the # key to commit your address change.

Table 79 LUI Menu Items (continued)

Menu Option	Description
6 VCX Config Menu	**Note**: See menu option 7 VCX Config Menu for information about how to access this option on 3101B and 3102B Business Telephones. Not used in an NBX environment. 3Com telephones can operate as SIP clients for the 3Com VCX Telephone System. This option opens a submenu that allows you to set telephone operating settings for a VCX environment.
6 Advanced Settings	***On 3101B and 3102B Business Telephones only:*** **1 Set NCP MAC Addres**s — Lets you specify the MAC address of the Call Processor. In all but special circumstances, the system messages communicate this information and you do not need to manually configure the MAC address. To change a telephone back to its default setting, enter all Fs for the Call Processor MAC address. **2 Show EEPROM Contents** — Lets you scroll through the locations in the memory of the telephone. The information is presented in hexadecimal format and can be properly interpreted only by a 3Com service person. **3 Set EEPROM - Default** — Restores the telephone to default settings by clearing these configured settings: ■ **IP Information** — My IP, Subnet Mask, Gateway IP, NCP-IP, and the Alt Download Server IP return to 255.255.255.255. ■ **NCP MAC address** — The Call Processor MAC address returns to ff:ff:ff:ff:ff:ff. ■ **SIP Parameters** — All SIP specific parameters will be set to default 0xffff (data parameters) or 255.255.255.255 for IP addresses. **NOTE:** If you select this option you are prompted to verify your action before the system clears the EEPROM

Table 79 LUI Menu Items (continued)

Menu Option	Description
	4 Forced Operations SW Upgrade — Resets the device. You can perform the same task by removing power from the telephone. Forces the telephone to retrieve an image from the downloader. **5 Hardware Reset** — Resets the telephone and starts with the bootstrap code. **6 Ping H3/IP** — Runs an H3 IP ping test. See Using H3PingIP for more information. **7 Test - LED & LCD** — Turns on all LEDs for 5 seconds, then fills every pixel on the display panel for 5 seconds. **8 Test - Buttons** — Puts the telephone in the button test state. Press any telephone button to see a description of the button's function. To return to the main menu, press the pound (#) button ***twice***: **9 Audio Collection** — Allows user to specify a PC address to store audio packets when the user is on call. Used to debug audio quality issues that might arise in the field.
7 Reserved	Reserved for future use (except on 3101B and 3102B Business Telephones).
7 VCX Config Menu	***On 3103B and 3102B Business Telephones only:*** Not used in an NBX environment. 3Com telephones can operate as SIP clients for the 3Com VCX Telephone System. This option opens a submenu that allows you to set telephone operating settings for a VCX environment.
8 Test LED & LCD	**Note**: See menu option 6 Advanced Settings for information about how to access this option on 3101B and 3102B Business Telephones. On all 3Com Business Telephones and 3Com 3101 and 3101SP Basic Telephones, turns on all LEDs for 5 seconds, then fills every pixel on the display panel for 5 seconds. On all 3Com Basic Telephones, turns on the icons and words on the right side of the display panel for 5 seconds. Icons: Telephone icon plus the number 1 (top line) and telephone icon plus the number 2 (bottom line) Words: FWD (top line) and IN (bottom line).
8 Diagnostics	***On 3103B and 3102B Business Telephones only:*** Runs diagnostics. This option requires a password.

Table 79 LUI Menu Items (continued)

Menu Option	Description
9 Test – Buttons	**Note**: See menu option 6 Advanced Settings for information about how to access this option on 3101B and 3102B Business Telephones. Puts the telephone in the button test state. Press any telephone button to see a description of the button's function. To return to the main menu, press the menu button ***twice***: ■ On 3102 Business Telephones:  ■ On 1102, 2102, or 2102-IR Business Telephones*:*  ■ On 3101 or 3101SP Basic Telephones or 3103 Manager's Telephones:  ■ On 2101 Basic Telephones:  ■ On 3106C or 3107C Cordless Telephones, *****.
0 EEPROM-Default	**Note**: See menu option 6 Advanced Settings for information about how to access this option on 3101B and 3102B Business Telephones. Restores the telephone to default settings by clearing these configured settings: **IP Information** — My IP, Subnet Mask, Gateway IP, NCP-IP, and the Alt Download Server IP return to 255.255.255.255. **NCP MAC address** — The Call Processor MAC address returns to ff:ff:ff:ff:ff:ff. **SIP Parameters** — All SIP specific parameters will be set to default 0xffff (data parameters) or 255.255.255.255 for IP addresses. **NOTE:** If you select this option you are prompted to verify your action before the system clears the EEPROM.

Table 79 LUI Menu Items (continued)

Menu Option	Description
AB1 Set NCP MAC **NOTE:** This setting is for test networks only.	**Note**: See menu option 6 Advanced Settings for information about how to access this option on 3101B and 3102B Business Telephones. Lets you specify the MAC address of the Call Processor. In all but special circumstances, the system messages communicate this information and you do not need to manually configure the MAC address. To change a telephone back to its default setting, enter all Fs for the Call Processor MAC address.
AB2 Show EEProm	**Note**: See menu option 6 Advanced Settings for information about how to access this option on 3101B and 3102B Business Telephones. Lets you scroll through the locations in the memory of the telephone. The information is presented in hexadecimal format and can be properly interpreted only by a 3Com service person.
AB3 Ping H3/IP	**Note**: See menu option 6 Advanced Settings for information about how to access this option on 3101B and 3102B Business Telephones. Runs an H3 IP ping test. See Using H3PingIP for more information.
AB4 Reset Phone	**Note**: See menu option 6 Advanced Settings for information about how to access this option on 3101B and 3102B Business Telephones. Resets the device. You can perform the same task by removing power from the telephone. However, Option AB4 can be useful for cordless phones, which cannot easily be disconnected from power.

The 3Com Telephone Local Configuration Application

You can manually configure most 3Com telephones using the telephone Local User Interface (LUI) utility to define the settings the device needs to communicate with the Call Processor. For the 3100 Entry Telephone, which does not have a display panel to show configuration information, use the 3Com Telephone Local Configuration application (TLC).

The TLC application enables you to specify the information that a device requires to communicate with the Call Processor over a routed network without using DHCP. You must still use the Auto Discover feature or manual configuration through the NBX NetSet utility to add the device to the system database.

Installing the 3Com TLC Application

The 3Com Telephone Local Configuration application is a Windows program that you install and run from a PC.

To install the 3Com Telephone Remote Configuration application:

1. Insert the NBX Resource Pack DVD into your DVD drive. If the autorun program does not start the DVD browser program, navigate to the DVD and start autorun.exe.
2. Click *NBX Applications* and then click *Telephone Local Configuratio*n.

   The installation program creates a shortcut on your Start menu that you can use to launch the 3Com Telephone Remote Configuration application.

Using the TLC Application

After you download and install the Telephone Remote Configuration application, use the Windows Start menu to launch it.

Follow these steps to use the TLC application to configure a 3Com device:

- Discover the 3Com device:
  - Connect the 3Com device to the same subnet as the PC that is running the TLC application.
  - Enter the device's MAC address (found on the label on the underside of the 3Com device) into the TLC interface.
- After the TLC application connects to the device, specify the device IP settings you want to assign.

After you configure a device, you can open the device list window again and configure another device. Note that the device list can include any 3Com device including switches and routers.

Using H3PingIP

You can use the H3PingIP menu item to ping another device on the network to test the telephone's connectivity and to check the packet delay.

When you use H3PingIP to test for connectivity, use the IP address of a device that is connected to the Call Processor. Do not use the Call Processor IP address. The 3Com Business Telephone uses the IP Gateway and subnet mask information programmed into it using the AB16 and AB17 buttons.

H3PingIP shows the following information:

- **Port** — The UDP Destination Port
- **Tx** — The number of packets transmitted
- **Rx** — The number of packets received
- **mS** — The delay time, in milliseconds

If you ping a device on a subnetwork different than the one on which the telephone is located, the delay time is greater.

System-level Troubleshooting

For each symptom listed in Table 80, perform the suggested actions in the order listed.

***WARNING:** Before you remove any component, **shut down the system software** and then turn off the power to the chassis by removing the chassis power cord. If the system has two power supplies, remove both power cords.*

Table 80 Troubleshooting Actions

Symptom	Possible Cause	Suggested Action
Date/time display on telephones is wrong, either incorrect date or shows random characters.	A power surge has corrupted the system time.	If the display shows incorrect date, use NetSet to reset the system time. If the display shows random characters, for example, 00; 0 #, you must: **1** Disconnect power to the chassis that holds the Call Processor. **2** Wait 60 seconds. **3** Reconnect power to the system. **4** Use NetSet to enter the correct date and time.
	Problem with Call Processor battery.	Contact your 3Com NBX Voice - Authorized Partner.
Your browser cannot find NetSet.	No IP connectivity	Verify that the computer you are using to run the browser has network connectivity. See "Establishing IP Connectivity" in the *NBX Installation Guide*.
	Routing problems	If your local IP environment includes a proxy server, you might need to reconfigure your browser parameters to ignore the proxy server. See the online Help for your browser.

Table 80 Troubleshooting Actions (continued)

Symptom	Possible Cause	Suggested Action
	Invalid IP configuration	The system has a default IP configuration that might need to be changed to match your local IP environment. Temporarily change the IP configuration of your computer so that the subnet configuration matches the system configuration. Specify 255.255.255.0 as the subnet and use IP address 192.168.1.191. After you change your computer's IP configuration, connect to the system and change its IP settings to match the IP environment of your local network. Change your computer's IP configuration back to its original settings, and then connect to NetSet using the new IP address. See "Establishing IP Connectivity" in the *NBX Installation Guide*.
Cannot open NetSet using the administrator username and password.	The CAPS LOCK key on your keyboard is activated.	NetSet username and passwords are case-sensitive. For example, NetSet accepts "administrator" but it rejects "Administrator" and "ADMINISTRATOR".
Callers on hold do not hear music.	No music source is connected to the Call Processor.	See "Adding External Hardware" in the *NBX Installation Guide* for more information.
	MOH audio is disabled.	Enable MOH audio in *System-Wide Settings*. See "Connecting a Music-on-Hold (MOH) Input Device" in the *NBX Installation Guide*.
	MOH volume is set too low.	See "Adjusting Music-on-Hold (MOH) Volume" in the *NBX Installation Guide*.
Lose date and time when rebooting the system.	Problem with the battery on the Call Processor.	See "Servicing the Network Call Processor Battery" on page 445.
NetSet is very slow in responding.	Your network uses a proxy server for Internet access.	A common networking practice is to employ a proxy server to shield your network from intrusion by unauthorized users. However, communications with NetSet do not need to pass through the proxy server. To speed access to NetSet, configure your browser to access the system without going through the proxy server.

Table 80 Troubleshooting Actions (continued)

Symptom	Possible Cause	Suggested Action
All greetings and prompts are missing. For example, calling the Auto Attendant or a user's mailbox produces silence instead of the expected greetings.	The wrong message compression format was selected.	Prior to R1.1.0, all audio used MuLaw compression. With R1.1.0, audio, that is, any prompt, message, or greeting, was recorded using ADPCM compression. If you are running R1.1.0 or higher, leave the compression format set to ADPCM. The ability to select the format allows you to migrate existing data into an older database for backwards compatibility. In release R2.6 and all later releases, the compression is set to ADPCM and you cannot change it.
Caller ID information is not appearing when an outside call arrives.	Your local telephone company is not providing Caller ID service to you.	Caller ID is typically an optional service which you must order from your telephone company. You might be able to see caller ID by number or by name (or both) depending on the service your telephone company provides.
	You are answering the telephone before the Caller ID information is fully received.	Caller ID information does not appear immediately. It usually appears between the first and second rings. If you answer the call too quickly, the information is never received. If you transfer the call, the person you transfer the call to sees your ID instead of the ID of the original caller.

Digital Line Card Troubleshooting

To troubleshoot a Digital Line Card correctly, determine whether the origin of the problem is:

- The hardware
- The software configuration
- The CSU (Channel Service Unit)
- The telephone company's line

To eliminate the Digital Line Card (T1 or E1) attach a loop back connector in place of the telephone company's line. Configure the card as described in the appropriate section of Chapter 5.

The 3C10116D T1 card and 3C101156D E1 card can respond to commands from the Central Office to loop back data at different points for diagnostic purposes. You enable each loopback test using the NBX NetSet utility. You initiate the Local and Framer loopback tests using the NBX NetSet utility. The Line and Payload loopback tests must be initiated

by the Central Office or by test equipment emulating Central Office equipment. For more information about how to enable loopback tests, see "Using Loopback Tests" on page 188.

After you complete the configuration, and with the loopback connector in place, verify that the Nominal status light (3C10165C E1 card or 3C10116C T1 card) on the front panel of the Digital Line Card is turned on (appears steady and green). For the 3C10165D E1 card and 3C10116D T1 card, make sure the CO status light is green.

- If the Nominal or CO status light does not turn on, the problem is most likely in the Digital Line Card. Contact your 3Com Voice-Authorized Partner to report the problem.
- If the Nominal or CO light turns on, the problem is either in the CSU (Channel Service Unit) or in the telephone company's line. Contact the telephone company for assistance.

The 3C10165D E1 Card and the 3C10116D T1 card each have an onboard CSU. You can view CSU statistics for the card through the NBX NetSet utility. For more information see "Viewing CSU State Information and Statistics" on page 185.

Alarm Conditions (Overview)

T1 and E1 Digital Line Cards might experience these alarm conditions:

- Red Alarm — Indicates one of these conditions:
  - Loss of Signal (LOS)
  - Loss of Framing (LOF) also known as Out of Frame (OOF)
- Blue Alarm — Indicates an Alarm Indication Signal (AIS)
- Yellow Alarm — Indicates a Remote Alarm Indication (RAI)

An alarm condition might be one of these:

- Signal — Information transmitted either in the upstream or downstream direction, warning of a detected failure:
- State — A condition, activated at a terminal device, indicating that a problem exists and remedial action is required.

T1 and E1 Digital Line Cards are considered "downstream" equipment.

Alarm Descriptions

Red Alarm

- **Carrier Fail Alarm** (Red CFA) — A state that exists at a downstream terminal device, based upon the terminal device detecting an incoming LOS or LOF.

Blue Alarms

- **AIS, Keep-alive/Blue** — A signal that is transmitted instead of the normal signal to maintain transmission continuity and to indicate to the receiving equipment that there is a transmission interruption either at the equipment that is generating the AIS signal or upstream of that equipment. The all ones signal is generated:
  - To maintain transmission continuity
  - To notify downstream equipment of a transmission fault
  - To indicate to downstream equipment that a DS1 framed signal is not being generated

  The transmission fault might be located at the equipment that is generating the alarm signal, or it might be located upstream of that equipment.
- **AIS CFA** (also known as Blue CFA) — A state that exists at the downstream equipment and indicates that it has detected an AIS signal from the upstream equipment.

Yellow Alarms

- **RAI** (also known as Yellow Alarm Signal) — A signal transmitted in the outgoing direction when a terminal determines that it has lost the incoming signal. The terminal equipment generates the Yellow Alarm Signal for a minimum of 1 second using one of these methods:
  - If you are using Super Frame (SF), the terminal equipment generates the Yellow Alarm Signal by setting the second bit in all channels of the Super Frame to 0 (zero).
  - If you are using Extended Super Frame (ESF), the terminal equipment generates the Yellow Alarm Signal by sending an alternating pattern of 8 ones followed by 8 zeros on the Facilities Data Link (FDL).
- **Yellow CFA** — A state that is activated at the terminal equipment when the terminal equipment detects a Yellow Alarm Signal. The Yellow Alarm Signal comes from the equipment at the other end

when the far end equipment enters a Red CFA state. See Red Alarm, earlier in this section.

Alarms on NBX Digital Line Cards

T1 and E1 Digital Line Cards support all of the alarm states and signals described in "Alarm Descriptions" on page 435. Table 81, next, and Table 82 on page 437 describe how the status lights indicate alarm conditions on Digital Line Cards.

Table 81 3C10165, 3C10165B, 3C10165C, 3C10116, and 3C10116C Status Lights and Error Conditions

Status Light	Purpose
Nominal	**On:** There are no error or alarm conditions. **Flashing:** A call is active on at least one channel.
CF (Carrier Fail)	**On:** A Red Alarm state or Blue Alarm state exists on the card. To determine which alarm state exists: **1** Log on to the NBX NetSet utility using the administrator ID and password. **2** Click *PSTN Gateway Configuration* > *Digital Line Cards*. **3** In the *Select Device Type* list, select *T1 Span List* or *ISDN PRI Span List,* and then click *Apply*. **4** Select the span you want and click *Status*. The words *Red Alarm* or *Blue Alarm* appear in the *Status* field.
RA (Remote Alarm)	**On:** A Yellow Alarm state on the card. To confirm that the Yellow Alarm state exists: **1** Log on to the NBX NetSet utility using the administrator ID and password. **2** Click *PSTN Gateway Configuration* > *Digital Line Cards*. **3** In the *Select Device Type* list, select *T1 Span List* or *ISDN PRI Span List,* and then click *Apply*. **4** Select the span you want and click *Status*. The words *Yellow Alarm* appear in the *Status* field. **NOTE:** This light is used only on the T1 Digital Line Card.
LB (Loop Back)	**On:** The card is in loop-back testing mode. **NOTE:** This light is not used to indicate any of the Red, Blue, or Yellow alarms.

Table 82 3C10165D and 3C10116D Status Lights and Error Conditions

Status Light	Purpose
CO	**Green:** There are no error or alarm conditions. **Amber:** An alarm condition at the remote end or the CO is not connected or available. To determine which alarm state exists: **1** Log on to the NBX NetSet utility using the administrator ID and password. **2** Click *PSTN Gateway Configuration* > *Digital Line Cards*. **3** In the *Select Device Type* list, select *T1 Spans* or *ISDN PRI Spans,* and then click *Apply*. **4** Select the span you want and click *Status*. The words *Red Alarm* or *Blue Alarm* appear in the *Status* field.

Configuration and Status Reports

You can obtain the status of all Digital Line Cards in the system with either of these two methods:

Select *PSTN Gateway Configuration* > *Digital Line Cards* and:

- Click *Config & Status Report*, which displays a formatted report with headings shown in a larger font in the window.
- Click *Export Report*, which displays an unformatted report in the window. To save the report as an ASCII text file, select *Save as* from the *File* menu of your browser.

Table 83 describes in alphabetical order (not the order of appearance) the headings in the Configuration and Status Report.

Table 83 Configuration and Status Report Headings

Heading	Description
#Chs	Number of channels.
#Dsp	Number of digital signal processors.
#OffChs	Number of channels in the offline state.
#OnChs	Number of channels in the online state.
AEClosed	Autoattendant extension when business is closed.
AELunch	Autoattendant extension when business is at lunch.
AEOpen	Autoattendant extension when business is open.
AEOther	Autoattendant extension for Other hours.

Table 83 Configuration and Status Report Headings (continued)

Heading	Description
ais	TEP performance data. Alarm Indication Signal. The number of seconds in which an ais was transmitted. An ais signal is transmitted in lieu of the normal signal to maintain transmission continuity and indicate to the receiving terminal that there is a transmission fault located either at the transmitting terminal or upstream of the transmitting terminal. Also referred to as a Blue Alarm.
aissp	TEP performance data. T1.231 Near End. Number of seconds when loss of frame encountered.
ANI	Automatic Number Identification. The telephone number from which the call originated.
Audio Input	Numeric value of audio input control setting.
Audio Output	Numeric value of audio output control setting.
Audio Compr	The type of audio compression selected for this span. Default means that the device is using the system-wide setting.
bbec	TEP performance data. G.826 Near End, Far End. Number of E1 background block errors.
bber	TEP performance data. G.826 Near End, Far End. Background block ratio.
bes	TEP performance data. Bursty Errored Seconds, TR54016 Far End and Far End. Number of seconds during which there were 2 to 319 CRC errors, but no Severely Errored Frame or AIS conditions.
BdId	Board (card) ID number.
BdId Name	Board (card) name.
Brd	The number of the board (card) in a multiple board system.
CO Switch Protocol	Protocol (ETS1, QSIG Slave) used by the CO switch (not applicable to T1).
Card Type	Type of card (T1, ISDN PRI, E1, BRI).
Ch MAC Address	Channel MAC address.
Ch List	Channels supported by a DSP.
Ch Name	Name of a channel.
ChId	Unique identifying number of a channel in a list of channels, possibly including channels from more than one board.
ChNo	Channel number. For example: 1–24 for a T1 board.
css	TEP performance data. Controlled Slip Seconds, TR54016 Near End and Far End. Number of seconds of controlled (benign) slips.

Table 83 Configuration and Status Report Headings (continued)

Heading	Description
cssp	TEP performance data. Controlled Slip Seconds Path, T1.231 Near End and Far End. Number of seconds of controlled (benign) slips.
CurState	Current state of a channel (in use, idle, available).
cv	TEP performance data. Code Violations, G.826 Near End. Number of bipolar violations and excessive zeroes.
cvl	TEP performance data. Code Violations Line, T1.231 Near End. Number of bipolar violations and excessive zeroes.
cvp	TEP performance data. Code Violations Path, T1.231 Near End and Far End. Number of bipolar violations and excessive zeroes.
datasecs	TEP performance data. The number of seconds with valid data.
DNIS/DID	Number of digits passed that identify the called party.
DSP Name	Name of a digital signal processor.
DSP Status	Status of a digital signal processor.
DSP Version	Version of code running on a digital signal processor.
Digit Collection	Specifies the data the CO sends and the format in which it is sent over the span of an incoming call. Can include both DNIS/DID and ANI, and can specify the order in which they arrive, and the number of digits involved.
EchoCanceller	The state of the echo cancellation function. Values: Enabled, Disabled.
E&M Direction	For a T1 line, the direction of the E&M signaling. Values: Two Way, One Way. Default: Two Way.
ErrorCnt	Reserved for future use.
ErrorCode	Reserved for future use.
es	TEP performance data. Errored Seconds, TR54016 Near End and Far End. Number of one-second intervals with exactly one CRC-6 error and no SEF or AIS defects.
esap	TEP performance data. Errored Seconds Type A, T1.231 Near End and Far End. Number of one-second intervals with exactly one CRC-6 error and no SEF or AIS defects.
esbp	TEP performance data. Errored Seconds Type B, T1.231 Far End. Number of one-second intervals with between 2 and 319 CRC errors.
esc	TEP performance data. Errored Seconds, G.826 Near End and Far End. Number of one-second intervals with exactly one CRC-6 error and no SEF or AIS defects.
esl	TEP performance data. Number of one-second interval with between 2 and 319 CRC errors. (line)

Table 83 Configuration and Status Report Headings (continued)

Heading	Description
esp	TEP performance data. Errored Seconds, T1.231 Near End and Far End. The number of one-second intervals with between 2 and 319 CRC errors.
esr	TEP performance data. Errored seconds ratio, G.826 Near End and Far End.
Ext.	The extension number for a channel.
fc	TEP performance data. Failure Count, T1.231 Near End and Far End. Total failure count for the sample.
FlashHookTransfer	Status of flash hook transfer function. If enabled, allows user receiving a call to do a flash hook transfer to another trunk line Values: Enabled, Disabled. Default: Enabled
Framing Type	Type of framing used on this board (ES4, D4). For a T1 board, ESF is always associated with a B8ZS line coding, and D4 is always associated with AMI line coding.
Framer Loopback	The state of the setting for the Framer Loopback test, either enabled or disabled.
GpId	Group ID number.
Group Name	Group name.
Guard	A time out value that controls the waiting period after a call completes, before the channel can be used for another outbound call from system.
InterfaceType	Type of interface. Values: E1, T1, ISDN, no config. Default: T1. Does not apply to T1 E&M.
Interval	TEP performance statistics are sampled every 15 minutes. The system saves up to 24-hours of data in 15-minute intervals.
Intl. Prefix	An advanced configuration setting. An identifier, up to five-digits, that can be manually configured for outgoing calls on this span. Manual configuration of the international prefix is for situations where the telephone company equipment requires special configuration on the system.
Line Code	Type of line coding used (HDB3, AMI). For a T1 board, AMI line coding is always associated with D4 framing, and B8ZS line coding is always associated with ESF framing.
Line Length	Length of the line between the termination and the board.
Line Loopback	The state of the setting for the Line Loopback test, either enabled or disabled.
lofc	TEP performance data. Loss Of Frame Count, T1.231 Near End and Far End. Number of Out-Of-Frame events.

Table 83 Configuration and Status Report Headings (continued)

Heading	Description
los	TEP performance data. Loss Of Signal Seconds, G.826 Near End. Number of seconds during which the signaling channel was lost.
lossl	TEP performance data. Loss of Signal Seconds, T1.231 Near End. Number of seconds during which no pulses (loss of signal) have arrived within 100 to 250 bit times.
Local Loopback	The state of the setting for the Local Loopback test, either enabled or disabled.
MAC Address	A 48-bit address unique to each network device.
Model Number	The model number of the board. **Values:** 0x0700 — T1 board 3C10116B 0x0b00 — T1 board 3C10116C 0x0e00 — T1 board 3C10116D 0x0c00 — E1 board 3C10165C 0x0f00 — E1 board 3C10165D 0x0a00 — BRI board 3C10164C
National Prefix	An advanced configuration setting. An identifier, up to five-digits, that can be manually configured for outgoing calls on this span. Manual configuration of the national prefix is for situations where the telephone company equipment requires special configuration on the system.
NCP Conne	The amount of time that the Digital Line Card waits for the Call Processor to connect the call. "USER_ALERTING_NO_ANSWER" errors mean that this value might be too small.
NCP Gener	A time-out value that controls how long the Digital Line Card waits for a response from the Call Processor. Do not modify this value.
Network Digit	A time-out value that controls how long the Digital Line Card waits between digits sent on an incoming call.
OffHk Min	The minimum time an analog telephone, connected to an Analog Terminal Card, must be off hook for the system to recognize that the telephone has been picked up.
On Line	One possible status of a channel.
oof	TEP performance data. Out of Frame Seconds, G.826 Near End. Number of seconds during which there were excessive frame bit errors.
Payload Loopback	The state of the setting for the Payload Loopback test, either enabled or disabled.

Table 83 Configuration and Status Report Headings (continued)

Heading	Description
Prepend Prefix	Full text: Prepend prefix to Calling Party Number in Setup Indication. Either enabled or disabled. National and international prefixes can be added for outgoing calls. The prefix is for situations where the telephone company equipment requires special configuration on the system.
Protocol	A signaling method used to make calls.
rai	TEP performance data. Remote Alarm Indicator, G.826 Near End and Far End. Number of seconds during which a remote alarm indication was declared.
Recv. Timer	Full Text: Overlap Receiving timer (T302). PRI span only. An advanced configuration setting for situations where the telephone company equipment requires special configuration on the system.
Release Complete	Full Text: Send "Release Complete" if incoming call is from incompatible equipment. Either enabled or disabled. An advanced configuration setting for situations where the telephone company equipment requires special configuration on the system.
RxWnkMax	The maximum duration of a received Wink signal.
RxWnkMin	The minimum duration of a received Wink signal.
sasp	TEP performance data. SEF/AIS Seconds, T1.231 Near End. Number of seconds when at least 2 frame bit errors or loss of frame encountered.
sefsp	TEP performance data. Severely Errored Frame Seconds, T1.231 Far End. Number of one-second intervals with either out-of-frame signals, AIS defects, 390 or more CRC errors, or four or more frame bit errors.
Sending Complete	Full Text: Send "Sending Complete IE" in Setup Request IE (Information Element) refers to the data fields within an ISDN layer 3 message. An advanced configuration setting for situations where the telephone company equipment requires special configuration on the system.
ses	TEP performance data. Severely errored seconds, TR54016 Near and Far End. Number of one-second intervals with either out-of-frame signals, AIS defects, 390 or more CRC errors, or four or more frame bit errors.
sesc	TEP performance data. Number of one-second intervals with either out-of-frame signals, AIS defects, 390 or more CRC errors, or four or more frame bit errors.

Table 83 Configuration and Status Report Headings (continued)

Heading	Description
sesl	TEP performance data. Severely Errored Seconds Line, T1.231 Near End. Number of one-second intervals with either out-f-frame signals, AIS defects, 390 or more CRC errors, or four or more frame bit errors.
sesp	TEP performance data. TEP performance data. Severely Errored Seconds Path, T1.231 Near End. Number of one-second intervals with either out-of-frame signals, AIS defects, 390 or more CRC errors, or four or more frame bit errors.
sesr	TEP performance data. Severely Errored Seconds Ratio, G.826 Near End and Far End.
Silence Suppr	The state of the silence suppression setting for this span. "Default" indicates that the span is set to use the system-wide setting.
SpId	Span ID.
SpNo	Span number.
Span MAC Address	MAC address assigned to this span.
Span Name	Name of span.
SpanNo	Identifying number for a span.
Start Type	Mechanism used to indicate start of a call.
Status	Status of a channel, span, card. Values: Online, Idle, Unknown. Default: Online
Strip #	Full Text: Strip trailing # from Called Party Number in Setup Request. Either enabled or disabled. An advanced configuration setting for situations where the telephone company equipment requires special configuration on the system.
TEI	Terminal Equipment Identification number (of BRI board). The telephone company might provide this number or the system might assign it, depending on how you purchased the BRI lines.
TEP Version	The version of software running on the board.
Time Last Seen	Last time activity was recorded for this board.
Timing Mode	Internal: Timing is generated from within the Digital Line Card. Loop: Timing is taken from the central office.
Trunk to Trunk	Whether call transfers are allowed from one trunk to another. Values: Enabled (default), Disabled, Restricted, Unrestricted.
TxGudMin	The minimum duration of a transmitted Guard signal.
TxWnkDura	The duration of a transmitted Wink signal.

Table 83 Configuration and Status Report Headings (continued)

Heading	Description
uas	TEP performance data. Unavailable Seconds, TR54016 Near End and Far End. Number of seconds during which the frame was unavailable for 10-seconds.
uasc	TEP performance data. Unavailable Seconds, G.826 Near End and Far End. Number of seconds during which the frame was unavailable for 10-seconds.
uasp	TEP performance data. Unavailable Seconds, T1.231 Near End and Far End. Number of seconds during which the frame was unavailable for 10-seconds.
vsecs	TEP performance data. Valid seconds for the selected interval.
Wink Wait	This time out value controls how long the Digital Line Card waits to respond with a wink signal on an outgoing call. If you see "no_wink_received" errors, this value might be too small.

Connecting a Computer to a Serial Port

On some devices, you can connect a computer to a serial port and, by running a terminal emulation program on the computer, you can obtain information about the status of the card or the system.

You can connect a computer directly to the serial port on these devices:

Table 84 Serial Port Connections

Card	Port
V3000 Call Processor	COM1
V5000 Call Processor	COM1
NBX 100 Call Processor	COM1
BRI-ST Digital Line Card	CONSOLE
E1 Digital Line Card	CONSOLE
T1 Digital Line Card	CONSOLE
Analog Line Card (3C10114C only)	CONSOLE
Analog Terminal Card (3C10117C only)	CONSOLE

It does not matter which computer operating system you use. As long as the computer has a terminal emulation program that can emulate a VT100 terminal (for example, Microsoft Hyperterminal), it can communicate with any of the cards listed in Table 84.

To connect the computer to the COM1 or CONSOLE port on a board:

1. Using a standard computer serial cable (9-pin male to 9-pin female), connect the male end of the cable to the female connector (COM1 or CONSOLE) on the front panel of the board.
2. Connect the female end of the cable to an available serial port on the computer.
3. Start the terminal emulation software and create a new connection.
4. Configure the connection to use the serial port to which you connected the cable and to use the settings in Table 85.

Table 85 Terminal Emulation Program Properties

Property	Value
Emulation	VT100
Baud Rate	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

All messages associated with the board (for example, the initialization process) appear in the terminal emulation window.

Servicing the Network Call Processor Battery

If you lose the system date and time when you reboot the V5000 system, it could mean that the Call Processor battery must be replaced. The battery is not a user-serviceable item. If you suspect a problem with the battery, contact your 3Com Technical Support representative.

WARNING: *There is a danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.*

Getting Service and Support

Your authorized 3Com NBX Voice-Authorized Partner can assist you with all your support needs, including systems and cable plant design, installation, configuration, and project management.

A choice of maintenance services, including remote diagnostics, on-site support, telephone technical support, and hardware replacement, is available from your 3Com NBX Voice-Authorized Partner. Training and enhancement services are also available.

A INTEGRATING THIRD-PARTY MESSAGING

The system can operate with a third-party messaging system. This appendix describes the steps that you must perform to use a third-party messaging system with the system:

- Installing Software on the Third-Party Messaging Server
- Configuring the System
- Configuring NBXTSP on the Server

If you are using the 3Com IP Messaging Module with a SIP -mode system, do not follow the instructions in this chapter. See the IP Messaging Module Installation Guide*, which is available through the NBX NetSet utility (click* Downloads > Documentation*).*

Installing Software on the Third-Party Messaging Server

You must install the NBX Media Driver and the NBX TAPI Service Provider (NBXTSP) on the third-party messaging server to enable it to interact with the system. See your messaging application's documentation for server requirements.

1. Install the NBX Media Driver application from the *NBX Resource Pack DVD* or the NBX Partner Access web site.
2. Install the NBXTSP software from the *NBX Resource Pack DVD* or the NBX Partner Access web site.

   You can also download the NBXTSP software from your system by connecting to the NBX NetSet utility from a browser located on the third-party messaging server.

Configuring the System

To activate third-party messaging on the system use the NBX NetSet utility to perform the tasks described in this section. All NetSet procedures require an administrator login.

1. Add the Third-party Messaging and Media Driver licenses to your system:
   - **a** Click *Licensing and Upgrades* > *Licenses* > *Add License*.
   - **b** In the *License Key* field, enter the license key provided by your 3Com Voice-Authorized Partner.
   - **c** Click *Apply*.
   - **d** Add any additional licenses. When you are finished adding licenses, click *OK*.
   - **e** Reboot the system.

3Com strongly recommends that you back up your licenses each time you make a license change.

2. Verify that Auto Discover Telephones is enabled:
   - **a** Click *System-Wide Settings* > *Auto Discovery*.
   - **b** Verify that *Auto Discover Telephones* is enabled.
   - **c** Click *Apply*.
3. Verify that NBX Messaging is disabled:
   - **a** Click *System-Wide Settings* > *Enable Features System-Wide*.
   - **b** Verify that *NBX Messaging* is disabled.
   - **c** Click *Apply*.
4. Create a Hunt Group for the third-party messaging system:
   - **a** Select *Call Distribution Groups* > *Hunt Groups* > *Add*.
   - **b** Set the following parameters:
     - **Name** — UM Hunt Group (or some similar name).
     - **Type** — HuntGroup - Circular.

3Com recommends that you use a circular hunt group.

   - **Extension** — Enter the appropriate extension for your hunt group.
   - **Password** — Set the password for this hunt group.
   - **Logout if no answer** — Verify that this check box is empty.

- **Users** — Select the WAV phones and the ATA ports that are connected to the third-party messaging system.
- **Call Coverage** — Set to voice mail.

c Click *Apply.*

5 Modify the Voice Mail Extensions List:

1 Click *Dial Plan > Extension Lists.*

2 Click **0003 VoiceMail* to display the Modify window.

3 To add a voice mail extension, use the Membership list:

a If the list does not include any voice mail extensions, click the check boxes next to the voice mail extension that you want to add to the list.

b If the list already has members, click *Show all* to display a list of voice mail extensions that you can add to the membership.

Note*: You can toggle between the Show all and Show members only buttons to display voice mail extensions that have membership in the list and the voice mail extensions that are not members of the list but which you can add to the list, and to confirm your changes.*

4 Click *OK*.

Configuring NBXTSP on the Server

On the third-party messaging server, you must add the WAV extensions to the NBX TAPI Control Panel. If your third-party messaging system needs TAPI messages from Analog Terminal Adapter devices or 3Com telephones, you must also add these devices to the NBX TAPI Control Panel.

Update the devices in the NBX TAPI Control Panel:

1 **WinNT** — On the server, select *Control Panel > Telephony > Telephony Drivers > NBX TAPI Service Provider.*

Win2K — On the server, select *Control Panel > Phone and Modem Options > Advanced > NBX TAPI Service Provider.*

2 Click *Configure* and add the extension numbers.

3 Click *OK*.

You are now ready to install your third-party messaging software. See your application's documentation for installation and configuration instructions.

B ISDN Completion Cause Codes

This appendix lists the Completion Cause Codes displayed in the Digital Line Card span *Status* windows.

To access the Status window:

1. Click the appropriate link:
   - *PSTN Gateway Configuration > T1 Spans*.
   - *PSTN Gateway Configuration > ISDN PRI Spans*.
   - *PSTN Gateway Configuration > ISDN BRI Spans*.
2. Click a span's state to display the *Status* window.

Table 86 lists the codes that detail the reasons for the termination of a call. Also, see "Configuring and Managing Digital Line Cards" on page 162 for more information.

These completion cause code descriptions are only guidelines. The detailed cause might vary according to the Public Switched Telephone Network (PSTN) to which your system is connected.

Table 86 Completion Cause Codes

Class Grouping	Hex Code	Decimal Code	Description	Details
Normal events	0x00	0	No diagnostic	
	0x01	1	Unassigned number	The requested destination, although valid, cannot be reached.
	0x02	2	No route	The sending equipment (sending the cause) is requested to route the call through an unrecognized transit network.
	0x03	3	No route to destination	The called user cannot be reached because the network does not serve the destination.
	0x06	6	Channel unacceptable	The last identified channel is not acceptable to the sending entity.

Table 86 Completion Cause Codes (continued)

Class Grouping	Hex Code	Decimal Code	Description	Details
	0x07	7	Call awarded	The incoming call is connected to a channel already established for similar calls (for example, packet-mode X.25 virtual calls).
	0x10	16	Normal clearing	This call is being cleared by one of the users involved.
	0x11	17	User busy	The called user cannot accept another call although compatibility is established.
	0x12	18	No user responding	The user does not respond to call establishment messages with either an alerting or connect indication within the allowed time.
	0x13	19	User alerting no answer	The user has provided an alerting indication but no connect indication within the allowed time.
	0x15	21	Call rejected	Equipment sending the cause does not wish to accept this call although it is not busy or incompatible.
	0x16	22	Number changed	The called party number is not assigned.
	0x1A	26	Non-selected user clearing	The user has not been awarded the incoming call.
	0x1B	27	Destination out of order	The destination interface is not operating correctly.
	0x1C	28	Invalid number format	The called party number is invalid, or incomplete.
	0x1D	29	Facility rejected	The network cannot provide the facility requested.
	0x1E	30	Response to status enquiry	The reason for the STATUS message was the prior receipt of a STATUS ENQUIRY message.
	0x1F	31	Unspecified cause	Used to report normal events only when no other cause in the normal class applies.
Resource unavailable	0x22	34	No circuit available	An appropriate circuit or channel is not currently available to manage the call.
	0x23	35	Call queued (AT&T)	The network is not functioning. Immediate redial is unlikely to be successful.
	0x26	38	Network out of order	The network is not functioning. Immediate redial is unlikely to be successful.
	0x29	41	Temporary failure	The network is not functioning. Immediate redial is unlikely to be successful.
	0x2A	42	Network congestion	The switching equipment generating this cause is experiencing a period of high traffic.

Table 86 Completion Cause Codes (continued)

Class Grouping	Hex Code	Decimal Code	Description	Details
	0x2B	43	Access info discarded	The network could not deliver access information to the remote user as requested. May include the type of discarded information (user-to-user information, low layer or high layer compatibility, or sub-address).
	0x2C	44	Requested channel not available	Returned when the circuit (or channel) indicated by the requesting entity cannot be provided by the other side of the interface.
	0x2D	45	Pre-empted	
	0x2F	47	Resources unavailable – unspecified	Reports a resource unavailable event only when no other cause in the resource unavailable class applies.
Service or option not available	0x31	49	Quality of service unavailable	Throughput or transit delay cannot be supported and that the Quality of Service (as defined in Recommendation X.213) cannot be provided.
	0x32	50	Facility not subscribed	The requested supplementary service could not be provided by the network because the user has not completed the necessary administrative arrangements with its supporting networks.
	0x34	52	Outgoing call barred	
	0x36	54	Incoming call barred	
	0x39	57	Bearer capability not authorized	The user is trying to make unauthorized use of equipment providing a bearer capability.
	0x3A	58	Bearer capability not available	The user has requested a bearer capability, which is implemented by the equipment generating the cause, but is not available at this time.
	0x3F	63	Service not available	Reports a service (or option) not available event only when no other cause in the service (or option) not available class applies.
Service or option not implemented	0x41	65	Capability not implemented	The equipment sending this cause does not support the requested bearer capability.
	0x42	66	Chan not implemented	The equipment sending this cause does not support the requested channel type.
	0x45	69	Facility not implemented	The equipment sending this cause does not support the requested supplementary service.
	0x46	70	Only restricted digital available	One equipment has requested an unrestricted bearer service but the equipment sending this cause only supports the restricted version.

Table 86 Completion Cause Codes (continued)

Class Grouping	Hex Code	Decimal Code	Description	Details
	0x4F	79	Service not implemented, unspecified	Reports the service (or option) not implemented event only when no other cause in the service (or option) not implemented class applies.
Invalid message	0x51	81	Invalid call reference	The equipment sending this cause has received a message with a call reference that is not currently in use on the user network interface.
	0x52	82	Chan does not exist	The equipment sending this cause has received a request to use a channel that is not activated on the interface for a call.
	0x53	83	Suspended call exists, call identity does not	A call resume has been attempted with a call identity that differs from that in use for any currently suspended calls.
	0x54	84	Call identity in use	The network has received a call suspended request that contained a call identity (including the null call identity) that is already in use for a suspended call within the domain of interfaces over which this call might be resumed.
	0x55	85	Incompatible destination	
	0x58	88	Incompatible destination	The equipment sending this cause has received a request to establish a call that has low layer compatibility, high layer compatibility, or other compatibility attributes (for example, data rate) that cannot be managed.
	0x5B	91	Transit network does not exist.	
	0x5F	95	Invalid message (unspecified)	Reports an invalid message event only when no other cause in the invalid message call applies.
Protocol error	0x60	96	Mandatory IE missing	The equipment sending this cause has received a message that is missing an information element that must be present in the message before that message can be processed.
	0x61	97	Nonexistent message	The equipment sending this cause has received a message with a message type that it does not recognize, either because it is an undefined message, or it is defined but not implemented by the equipment sending the cause.
	0x62	98	Wrong message	The equipment sending this cause has received a message that it considers as not permitted while in the call state; or a STATUS message was received indicating an incompatible call state.

Table 86 Completion Cause Codes (continued)

Class Grouping	Hex Code	Decimal Code	Description	Details
	0x63	99	Bad info element	The equipment sending this cause has received a message that includes information elements not recognized because the information element identifier is not defined, or it is defined but not implemented by the equipment sending the cause. However, the information element is not required to be present in the message to enable the equipment sending the cause to process the message.
	0x64	100	Invalid element contents	The equipment sending this cause has received an information element that it has implemented. However, the sending equipment was not able to implement the code because one or more of the fields were incorrectly coded.
	0x65	101	Wrong message for state	The received message is incompatible with the call state.
	0x66	102	Timer expiry	A timer has expired and an associated Q.931 error handling procedure has been initiated.
	0x67	103	Mandatory IE length error	
	0x6F	111	Protocol error	Reports an error event only when no cause in the protocol error class applies.
Interworking	0x7F	127	Interworking unspecified	There has been interworking with a network that does not provide cause codes for its actions. Therefore, the precise cause for a message being sent is not known.

C CONFIGURING OPTION 184 ON A WINDOWS 2000 DHCP SERVER

Overview

RFC 2132 (DHCP Options and BOOTP Vendor Extensions) allows for vendor-specific extensions to the DHCP protocol. It defines that option codes in the range 128 through 254 are set aside for site-specific extensions.

3Com telephones can receive their IP configuration from a DHCP server. However, 3Com telephones need configuration information that is not part of a standard DHCP response. You can use DHCP option 184 to specify this extended information:

- NCP IP Address — Each telephone must receive a download of operating settings from the Call Processor.
- Alternate Server IP Address — Specifies a second location from which a telephone can receive its download. (Not used in an NBX system.)
- Voice VLAN Configuration — Reserved for future use.
- Fail-Over Call Route Point — Reserved for future use.

This appendix includes an example of how to configure option 184 on a Windows 2000 server that has been configured to run DHCP server software. It describes these topics:

This appendix describes how to configure the Call Processor IP address only. The extended options are not used in an NBX environment. The information in this appendix pertains only to a Windows 2000 server. The configuration instructions differ for other DHCP servers. This appendix describes only the configuration of option 184, not how to install or perform basic configuration of the Windows 2000 server.

Creating Option 184

If you are configuring more than one subfield for Option 184, the first subfield must be the Call Processor IP Address for backward compatibility.

1. Start the DHCP Microsoft Management Console:

   Start > Programs > Administrative Tools > DHCP

   The *DHCP* dialog box appears. In the left pane, look for the name of your Windows 2000 DHCP server.

2. Right click the name of your DHCP server. From the menu that appears, select *Set Predefined Options* to open the *Predefined Options and Values* dialog box.
3. Click *Add* to open the *Option Type* dialog box.
4. In the *Name* field, type a name of your choice.
5. From the *Data Type* drop-down list, select *Byte*.
6. Enable the *Array* check box.
7. In the *Code* field, type *184*.
8. In the *Description* field, enter a description of your choice. Example: *NBX NCP IP Address*.
9. Click *OK*.

   In the *Predefined Options and Values* dialog box, the DHCP Microsoft Management Console creates a new option name by combining the option number with the name that you chose and adds this name to the *Option name* drop-down list. Example: If you used NBX as the option name, the system adds *184 NBX* to the drop-down list.

Editing Option 184 Values

1. Select the new option name from the *Option name* drop-down list, and click *Edit Array*. The *Numeric Value Array Editor* dialog box appears.
2. In the *Data entry* area of the dialog box, click the *Decimal* radio button at the right of the word *Format*.
3. In the *Current Values* field, highlight the 0 (zero), and click *Remove*.
4. To create the new value, enter each element of the new value:
   a. Click in the *New value* field.
   b. Type the individual element value.

c Click *Add*.

5 Repeat steps 4 a, b, and c for each element in the following table. As you add each element, it appears in the *Current values* list, above previously added values.

Add these elements in this order:

Table 87

What You Type	Description
1	Enter 1 as the only suboption code for option 184. (Some options can have more than one suboption.)
4	The length of the argument that applies to this suboption. For option 184, suboption 1, the argument is an IP address, which is composed of four numerical fields (octets).
NOTE: *The next four fields use 10.234.1.254 as the sample IP address of the Call Processor. Enter the IP address of your Call Processor.*	
10	The first octet in the IP address of the Call Processor.
234	The second octet in the IP address of the Call Processor.
1	The third octet in the IP address of the Call Processor.
254	The fourth octet in the IP address of the Call Processor.

6 After you have entered all elements in the new value, click *OK*. You return to the *Predefined Options and Values* dialog box. The values that you entered appear in the *Value* area of the dialog box under *Byte*.

The values appear in hexadecimal format although you entered them in decimal format.

7 To accept the values, click *OK*. You return to the *DHCP Microsoft Management Console* dialog box.

Activating Option 184

To activate option 184, decide whether you want to apply the option to a specific scope or globally, that is, to all scopes that are served by the DHCP server software.

To activate option 184 for a specific scope:

1 In the left pane of the *DHCP Microsoft Management Console* dialog box, find the scope that you want. Then highlight *Scope Options*.

2 Right click *Scope Options*, and, from the menu that appears, select *Configure Options*. The *Scope Options* dialog box appears.

3 Scroll down in the *Available Options* list until you find the option that you just added (*184 NBX* in this example).

4 Enable the check box to the left of the option.

5 Click *OK*.

In the right pane, the option name now appears in the *Option Name* column. The *Vendor* column contains the word *Standard*. The values of the individual elements that you entered appear in the *Value* column.

The values appear in hexadecimal format although you entered them in decimal format.

To activate option 184 globally:

1 In the left pane of the *DHCP Microsoft Management Console* dialog box, highlight *Server Options*.

2 Right click *Server Options*, and from the menu that appears, select *Configure Options*. The *Server Options* dialog box appears.

3 Scroll down in the *Available Options* list until you find the option that you just added (*184 NBX* in this example).

4 Enable the check box to the left of the option.

5 Click *OK*.

In the right pane, the option name now appears in the *Option Name* column. The *Vendor* column contains the word *Standard*. The values of the individual elements that you entered appear in the *Value* column.

The values appear in hexadecimal format although you entered them in decimal format.

D CONNEXTIONS H.323 GATEWAY

This appendix provides information about how to install and configure the 3Com ConneXtions H.323 Gateway.

It describes these topics:

Overview of ConneXtions

ConneXtions is a 3Com software product that allows you to use an appropriately configured Windows system as an H.323 gateway for use with NBX systems.

H.323 gateways implement an ITU standard that allows telephone-like call connections to occur through an IP network. Although this standard addresses the means for transferring data, voice, and images, the NBX ConneXtions H.323 Gateway focuses on delivering low-cost, high-quality, voice connections through IP networks.

The ConneXtions software adapts internal system protocols to equivalent H.323 protocols that are carried across a WAN in IP packets. The H.323 protocol addresses:

- Negotiated connections.
- Negotiated voice compression.
- Standard extensions.
- Remote Internet device connections.

For more information, see "Overview of H.323" on page 471.

Installation Requirements

The ConneXtions H.323 Gateway software requires a system and at least four additional components:

- A router with access to a wide area network (WAN)
- A Windows-based server connected to the NBX LAN
- ConneXtions software (on the *NBX Resource Pack CD*)
- A ConneXtions license

Systems that receive H.323 calls through the public Internet might also need a firewall. See "Firewall Security" page 480.

WAN Router

WAN Routers typically connect to ISDN, T1, E1, Frame Relay, or Asynchronous Transfer Mode facilities, depending on the load they carry.

A dedicated router can often reduce problems encountered with firewalls. Firewalls often interfere with connections because they are designed to admit only authorized addresses, and because they discriminate against specific types of packets. The unusual complexity of the H.323 protocol presents special problems for firewalls because it requires additional processing. To minimize packet delay through a firewall, verify that the firewall is configured to give H.323 packets a high processing priority.

During installation, you can select a range of TCP or UDP ports to use with H.323 connections to provide more flexibility when using firewalls.

A ConneXtions gateway can use a separate network interface card to bypass the firewall delay. However, implement this solution only if it is

consistent with your company's network security policy. For more information, see "Firewall Security" on page 480.

Windows-based System

The ConneXtions software requires a dedicated computer system that is running Windows 2000. The system hardware must be certified by Microsoft. The installation software checks for the presence of Windows 2000 and then loads the correct packet driver from the *NBX Resource Pack CD*.

Although the ConneXtions software requires little disk storage, processing and memory requirements are crucial, and you might need multiple gateways. Microsoft server licenses do not apply because no additional operating system logons are involved.

The main considerations are "Windows Compatibility" and "Processor, Memory, and Bandwidth Requirements", discussed next, and "Firewall Security", on page 480.

Windows Compatibility

To check the compatibility of your system:

1. On a computer that has Internet access, enter `www.microsoft.com/hwdq/hwtest`
2. Locate the link to the Hardware Compatibility List.
3. Verify that your intended Windows 2000 system is on the Hardware Compatibility List.

Processor, Memory, and Bandwidth Requirements

Each G.711 call needs about 50 MHz on a Pentium II or 20 Mhz on a Pentium III. Each G.723 call needs about 128 MHz on a Pentium II or 75 Mhz on a Pentium III. These speed requirements increase directly with the number of ports. The IP router bandwidth requirements also increase directly with the number of ports.

The bandwidth requirements for a Pentium II and a Pentium III are identical.

Table 88 shows the speed and bandwidth requirements for different numbers of ports. It assumes that each packet carries a 50-byte overhead.

Table 88 Pentium Processor Capabilities

	Pentium II Speed (MHz)		Pentium III Speed (MHz)		Bandwidth (Kbps) on the LAN	
Ports	**G.711**	**G.723**	**G.711**	**G.723**	**G.711**	**G.723**
2	100	256	40	150	153.6	38.4
4	200	512	80	300	307.2	76.8
8	400	1000	160	600	614.4	153.6
16	800	2000	320	1200	1228.8	307.2
32	1600	4000	640	2400	2457.6	614.4
64	3200	10000	1280	4800	4915.2	1228.8
100	5000	12800	2000	7500	7680	1920

The memory requirements to support port processing also increase with each new port. A fully configured system, with the maximum number of ports (100), needs 600 MB of main memory. Hard disk requirements are less than 40 MB.

Table 89 lists the theoretical maximum number of ports that typical Pentium processors can manage.

Table 89 Pentium II and III Processor Capabilities

Pentium II	Ports		Pentium III	Ports	
(MHz)	**G.711**	**G.723**	**(MHz)**	**G.711**	**G.723**
300	6	2	450	22	6
400	8	3	500	25	6
500	10	4	533	26	7
600	12	4	550	27	7
650	13	5	600	30	8
Dual 500	20	8	650	32	8
			667	33	8
			700	35	9
			733	36	9
			750	37	10
			800	40	10
			1500	74	20

The maximum number of ports can be limited by the number of licenses.

If your port processing requirements exceed the capacity of a single processor, ConneXtions software supports either multiprocessor (dual and quad Pentium processors) or multiple gateway solutions. A Windows 2000 system that uses a dual 800 MHz Pentium processor achieves the same result.

Other System Requirements

Each H.323 port requires 6 MB of memory. 3Com recommends a PC with at least 128 MB of memory. Disk storage requirements are minimal. In addition to memory and disk storage, the operating system needs:

- A compact disk drive for loading ConneXtions software from the *NBX Resource Pack CD*.
- A 3Com Network Interface Card for connecting to the NBX LAN (10BASE-T or 100BASE-T).
- A 3Com Network Interface Card for connecting to a separate firewall or router (optional).

  The Call Processor coordinates its activities with the gateway through a Network Interface Card (NIC) in that gateway system. The same NIC can also be used to communicate with the IP router. This single NIC configuration is appropriate if the firewall, which separates Internet and intranet, is either unnecessary or is required by company policy.

ConneXtions Software

You use the *NBX Resource Pack DVD* to install ConneXtions software. The ConneXtions software performs the protocol conversions between a system and the international H.323 standards. To a system administrator, H.323 ports look like PSTN line ports. Both have extensions and are configured the same way but have different license requirements.

The NBX Resource Pack DVD *is also required to change H.323 gateway parameters after installation. A dealer who wants to explore possible hardware incompatibilities by running ConneXtions from a substitute laptop must reinstall ConneXtions on the laptop at each site.*

Preparing for Installation

Before you install a ConneXtions H.323 Gateway:

- Assemble system information.
- Check for the G.723 convertor (optional).
- Verify and install the NT Service Pack (Service Pack 4) (if required).

- Assemble permissions, licenses, and notifications.

Do not uninstall the current version. You would remove the current settings.

Assembling System Information

ConneXtions is installed through an InstallShield wizard. It presents a series of dialog boxes that request specific permissions and configuration information. Assemble this information before you begin an installation:

- Administrator login name: **<administrator>**
- Administrator password: **<xxxxxxxxx>**
- NBX H.323 software and associated port licenses.
- Caller ID label for outgoing calls. The default is the caller's extension. Use the main office telephone number (10 digits in the United States).
- The system name. Supply the name that H.323 callers see when they connect to the Auto Attendant.
- The TCP or UDP port ranges for use with a firewall, if any.

Verifying the G.723 Converter

Installations that need G.723.1 audio compression require access to a converter in Microsoft NetMeeting 2.1 or 3.01. NetMeeting must be installed on the same PC that holds the ConneXtions software, but the two cannot run simultaneously.

G.723.1 does not appear as a selectable option in ConneXtions unless the converter is accessible.

To confirm that the convertor is present, search for the `msg723.acm` file on your hard drive or download it from the Microsoft web site.

Configuring Licenses

To configure licenses, enter system information, such as the number of H.323 ports that you want to install. You can find this information through NetSet.

You can purchase licensed keycodes to unlock additional ports. A license provides a software key that unlocks ports that are already loaded. You can purchase licenses to enable or upgrade a system to:

- 1, 2, 4, 8, 16, 32, 64 or 100 ports on a V3000, V3001R, or V5000 system
- 1, 2, 4, 8, or 16 ports on an NBX 100 system

Software keys are tied to the system serial number.

To configure licenses:

1 Log on to NetSet:

   a Open your browser and connect to the Call Processor by using its IP address (example: 192.168.1.190) or host name (example: Home).

   b Click *Administrator.*

   c Enter your username and password.

   d Click *OK.*

2 **Access and record the Call Processor MAC address:**

   a In the NBX NetSet - *Main Menu* window, click *Reports*.

   b Click the *System Data* tab.

   c Record the MAC address.

MAC addresses use colons as separators. Take care to record the Call Processor MAC Address, not the Music-on-Hold MAC address, which also appears in the System Data tab.

3 **Determine the number of port licenses:**

   a In NetSet, click *Licensing and Upgrades* > *Licenses*.

   b Record the number of licenses for the H.323 Gateway.

   c Click *Add License.*

   d Enter the License Key (must be purchased) to unlock the license. To obtain a license key, contact 3Com order management or your supplier.

   e Click *OK.*

Do NOT click Apply. If you click Apply and then OK, the system warns you that you have an invalid license.

4 **Specify Auto Discovery:**

   a Click *System-Wide Settings.*

   b Check *Auto Discover Line Cards.*

   c Click *OK*.

Installing ConneXtions

To install the NBX ConneXtions H.323 Gateway:

1. Insert the *NBX Resource Pack DVD* into the PC. Click *NBX Applications, and* then click *NBX ConneXtions,* and then click *OK.*

If the program does not start automatically, click the Windows Start menu, and then Run. Type D:autorun, substituting the letter of your DVD drive for D, and click OK.

2. Respond to these initial InstallShield dialog boxes:
   a. In the *Welcome* dialog, click *Next.*
   b. In the *License Agreement* dialog, click *Yes.*
   c. In the *Default Destination Location* dialog, click *Next* or browse for an alternative destination location.
   d. In the NBX license request dialog, click *Yes.* This confirms that the system is legal.
3. Specify the Audio Channel Format:
   a. Select first option (G.711 only) for uncompressed connections
   b. Select one of the other two options to configure G.723.1 connections.

   These options require the file `msg723.acm`. See "Verifying the G.723 Converter" on page 466.
4. Information Block - click *OK.*
5. Specify the number of configured H.323 ports for this ConneXtions gateway. 3Com recommends that licenses are allocated equally when using multiple gateways.
6. Optionally, specify a Caller ID Label by entering an outgoing caller ID notification label of up to 33 digits. Enter numbers only, no other characters or spaces.

   Example: **`9787490000`**

   (The Caller ID shows the caller's extension number followed by the `[User Name]` if the entry is left blank.)
7. Specify the Call Processor name. Enter the name H.323 callers see when they reach the Auto Attendant.
8. Only one Gateway? - Click *Yes* if the system has only one H.323 gateway system.

CAUTION: *Multiple gateways must have unique configurations. Multiple gateways need a distinguishing "Gateway Number". Assign the first installed gateway to number 0; the second to number 1; and so on. 3Com recommends that licenses be allocated equally when using multiple gateways.*

9 Enter the Call Processor MAC Address. To find it, log on as an administrator in NetSet, and click *Reports*, followed by the *System Data* tab.

Be sure to record the Call Processor MAC Address, not the Music-On-Hold MAC address, which also appears in the System Data tab.

10 Select the country in which you are using ConneXtions. This defines the tones and cadences that ConneXtions uses.

11 Specify the UDP and TCP port ranges for use with a firewall. If these ranges are not important in your system, use the default settings. You can coordinate these settings with the firewall administrator.

12 Do you want to interface with a Gatekeeper? Click *Yes* if you want to use a gatekeeper. Gatekeepers act as the central point for all calls within their zones and provide call control services to registered endpoints.

13 If you have chosen to use a gatekeeper, enter the IP address of the preferred gatekeeper. This forces ConneXtions to try to use this gatekeeper first and provides a more secure option. If you want ConneXtions to autodiscover a gatekeeper, leave the field empty. You might chose to do this if you only have one gatekeeper on your network.

14 Choose what you want ConneXtions to do if it cannot register with the preferred gatekeeper:

Autodiscover a new Gatekeeper — ConneXtions allows you to make direct H.323 (unregistered calls) while attempting to contact an alternative gatekeeper on the network.

Continue unregistered — ConneXtions continues to function without using a gatekeeper.

Block Calls — ConneXtions blocks calls if it cannot register with a gatekeeper. (You must either have a gatekeeper on the network, or select one of the other options which enables ConneXtions to work without a gatekeeper present.) If a gatekeeper becomes available, you must stop the ConneXtions service and then restart it.

15 Do you want to use alternate Gatekeepers? If you select *Yes*, the chosen gatekeeper maintains a list of alternate gatekeepers to be used if the preferred gatekeeper does not respond.

If you choose to use alternate gatekeepers and have also selected to autodiscover new gatekeepers if ConneXtions cannot contact the preferred gatekeeper, ConneXtions first tries to use alternate gatekeepers from the list (in priority order); if this fails, it then tries to autodiscover a new gatekeeper.

16 Do you want to route calls through the Gatekeeper? You can route H.323 calls through the gatekeeper for these reasons:

- To control calls more effectively. For example, service providers need to be able to control call flow to allow them to bill for calls placed through the network.
- To reroute a call to another endpoint if a called endpoint is unavailable.
- To maintain interoperability with multi-vendor equipment which routes all calls directly using the gatekeeper.
- To use address resolution in large multi-zone configurations which have one or more gatekeepers in each zone.

17 You are prompted to set the size of the log files. The default value is 1 Mb. ConneXtions maintains two log files, named `ConneXtions01.log` and `ConneXtions02.log`. Data is logged to only one of these at a time. Once the active log file reaches a specified size, data logging switches to the second log file. Any data previously stored in that log file is overwritten.

18 Setup Complete: Click *Finish*.

Finishing the Installation

Verify the installation:

1 Log on to NetSet using the administrator login ID and password.

2 Click *PSTN Gateway Configuration* > *Line Cards*.

3 Note the MAC Address, extension, status, and group for each port.

4 Record the extension numbers for each H.323 port.

5 Enter user-friendly port names that appear when a user dials an H.323 port.

6 Close the browser to exit NetSet and end the installation.

Overview of H.323

The H.323 standard provides a foundation for audio, video, and data communications across IP-based networks, including the Internet. By complying with H.323, multimedia products and applications from different vendors can interoperate, allowing users to communicate without concern for compatibility.

An NBX ConneXtions H.323 Gateway provides connections similar to tie lines between existing NBX systems across an IP network. However, it can also support voice connections between a 3Com Telephone and other H.323-compliant devices.

ConneXtions H.323 Gateways support communication with:

- Extensions on other NBX systems that have a ConneXtions gateway.
- Extensions on PBX systems that have an attached H.323 gateway.
- H.323 gatekeepers.
- Miscellaneous H.323-compliant end-point devices such as:
  - H.323 telephones.
  - Suitably equipped personal computers.
  - An emerging class of wireless handsets.

The quality of H.323 calls over the Internet is determined by the quality of the connection provided by your ISP.

The H.323 protocol addresses these main areas:

- Negotiated Connections
- Negotiated Voice Compression
- Standard Extensions
- Remote Internet Device Connections

Negotiated Connections

The H.323 protocol adds negotiated call setup and tear-down capabilities to Internet Protocol (IP) connections. It exists because Internet protocols were designed to deliver text messages and computer files in data packets. IP networks were not originally concerned about involving a person in a real-time conversation as a telephone does.

H.323 provides call setup capability to negotiate the readiness of two parties to exchange information and how they do it. It then keeps the

connection alive until one of the parties ends the connection. A call tear-down signal indicates to the network, and to the other party, when a call ends. On standard telephone networks, the telephone company uses this signal to determine when to start and stop charging for long distance calls, but long distance charges do not normally apply to H.323 calls. Other reasons for call setup and tear-down signals are to indicate when an IP network can release bandwidth to support other calls, and to inform other devices, such as voice mail systems, when to stop their conversation-related activities.

Negotiated Voice Compression

IP networks can carry a lot of traffic, creating competition for the available bandwidth. Devices have the best access, and the least delay, when they communicate messages by using fewer and smaller packets. This also means lower cost.

Voice compression offers a way to reduce the number and size of the data packets needed to carry each second of a voice conversation. However, voice compression needs high-speed processors to remove the redundancies that are inherent in the way standard voice is represented.

The international standard for representing voice (G.711) requires 64 Kb for each second of conversation. 3Com Business and Basic Telephones contain a digital signal processor (DSP) that transforms spoken voice into this form. An Ethernet interface, also within each telephone, breaks up the 64 Kbps stream into frames, adds addressing and error checking, and dumps the voice-data frames (now 83 Kbps) onto a 10 Mbps LAN. Elsewhere on the LAN (local or remote), the destination telephone detects its address, recovers the frames, extracts the bit stream, and reproduces the voice.

While LANs have enough bandwidth to support uncompressed digitized voice transfers, WAN bandwidth is less generous. For this reason, compression is often used to squeeze the digitized voice into a smaller bandwidth that can be carried across an Internet in smaller packets.

When an call passes through an H.323 gateway, the ConneXtions software performs an intermediate step that extracts the essential voice information, encapsulates it in packets, and sends it across an IP network.

G.723 is a compression standard that represents each second of voice conversation with 6.3 Kbps. ConneXtions software supports the use of this compression standard. With more than one way to represent voice

(G.711 and G.723), H.323 gateways negotiate the type of compression they use during each call setup. Negotiation ensures that the compression on the transmit side matches the decompression processing on the receiving side. With the frame and packet overhead, each G.723 channel needs about 19.2 Kbps of the available bandwidth.

Standard Extensions

ConneXtions routes incoming H.323 calls to one designated extension, usually the Auto Attendant. Callers can dial additional digits to redirect calls to internal extensions, but cannot access outside lines by dialing 9.

Remote Internet Device Connections

A system with a ConneXtions gateway can communicate with remote H.323 devices other than 3Com Business and Basic Telephones, such as:

- Wireless handsets
- Personal computers
- Ordinary telephones (POTS) with adapters
- H.323 gatekeepers

Wireless Handsets

An emerging class of H.323 wireless handsets is being used by some large outlet stores as portable PBX telephones. A ConneXtions H.323 server is well suited for use with these H.323 handsets.

Personal Computers

Microsoft NetMeeting software supports H.323 voice connections over the Internet. The personal computer must be equipped with Internet access, a sound system, and a microphone.

The current version of Microsoft NetMeeting (3.01) cannot conveniently place calls through the Auto Attendant because it has no way of entering extension digits after it reaches an IP address (the Auto Attendant). This is a temporary limitation that usually disappears when those programs upgrade to H.323 version 2. Version 2 requires that compliant devices support out-of-band DTMF (touch-tone) signaling.

If you choose ConneXtions as the gateway under the Advanced Calling options, and if you configure NetMeeting to "speed dial" the IP address and extension, Microsoft NetMeeting can place calls to an extension.

POTS Adapters

You can purchase circuit boards that plug into a personal computer and adapt an analog telephone (POTS) for use with an H.323 connection.

H.323 Gatekeepers

The gatekeeper is an H.323 entity on the network that provides address translation and controls access to the network for H.323 terminals, Gateways, and MCUs. The gatekeeper also provides services to the terminals, Gateways, and MCUs, such as managing bandwidth and locating Gateways.

The H.323 Connection

H.323 calls between local and remote 3Com Business and Basic Telephones are transparent to users, except for the IP dial plan. The Call Processor sets up the local end of the H.323 call as though it were setting up a call through a line card. However, this connection actually goes to a network interface card (NIC) in a dedicated Windows 2000 system that is running the ConneXtions software.

The Call Processor requests an H.323 port in the ConneXtions software by sending a frame, with a simulated Ethernet address, that contains a requested IP address. The ConneXtions gateway uses this address to request a level three connection between the local router and the remote router associated with another PBX or NBX system.

After an IP connection has been established, the ConneXtions software begins a series of H.323 exchanges by using TCP packets on the IP connection.

These H.323 exchanges set up the call and negotiate the type of voice compression that is used. They also cause the remote NBX (or PBX) system to begin setting up the remote end of the connection.

Connection Considerations

As soon as an end-to-end connection has been set up, all three networks (local LAN, WAN, and remote LAN) are ready to pass voice packets. The 3Com Business and Basic Telephones use their DSP to convert spoken words into digital voice packets. The voice packets are transferred across the Ethernet to the local H.323 gateway. The gateway strips off the Ethernet frames, compresses the voice, and encapsulates it within UDP packets which are delivered to the router, again via the Ethernet. The UDP packets are placed on the WAN for IP delivery to a remote H.323

gateway. The remote gateway undoes the process and sends the decompressed voice to an extension.

Connection considerations apply to two areas:

- Overall Connectivity
- Quality of Service

Overall Connectivity

An end-to-end H.323 connection consists of a succession of Physical Connections and Logical Connections, both local and external.

Physical Connections

An H.323 gateway has few *physical* connections. An installer can add an H.323 gateway to an existing system by creating one physical connection on the LAN that links a network interface card in an operating system to a hub or to a switch. The same connection also gives the H.323 gateway a direct connection to every other device on the near-end LAN. Those devices include any 3Com Business or Basic Telephone, the Call Processor, and the firewall or router.

Alternatively, you can use a second NIC in the gateway system to provide a separate connection between the H.323 gateway and the IP router.

Logical Connections

Locally, every device on an NBX LAN has the same physical access to the local network traffic as any other device. Consequently, addresses control connections because devices can only read information that is addressed to them. This makes addressing, and managing addresses, a key concern for logical continuity.

Logical continuity concerns extend throughout a network connection because the identity of a frame (or packet) and its destination determine where it goes, how it is managed, and what happens to it.

Because so many devices share the same physical media on the Internet and on the local network, there is always the possibility of incomplete or degraded connections that arise from network congestion, device configuration, or addressing problems.

Bridges, switches, routers, and firewalls can help to manage network congestion, conversions, and security. Configuration problems with of any of these devices can cause connection difficulties.

Bridges and switches are used to segregate areas of congestion within a local network (switches are multiport bridges). Routers perform a similar function but at the Layer-3 level where they perform conversions between LAN and WAN protocols. Firewalls, which are often built into routers, protect intranets from unauthorized internet users.

All of these devices can filter packets based on source address, destination address or packet type. Depending on how the devices are configured, they can let packets pass or they can block them.

Quality of Service

Unlike switched network connections, Internet voice connections consist of a sequence of numbered data packets. Packet transfers across the Internet are subject to delays or loss or both. If these delays are great (larger than 200 ms), or if the packet loss is excessive, voice quality deteriorates noticeably. The round-trip delay is typically no greater than 400 ms. You can test this by using several "ping" commands.

Voice conversations occur in "real-time," so these packets need to be delivered in a consistent manner and with the shortest delay. The goal is to deliver 32 regularly spaced packets to the recipient every second.

The frequency response, dynamic range, and noise of a voice conversation depend on the voice representation. If all data packets reach their destination, the system provides voice of a specified quality.

The H.323 standard accommodates alternative voice compression standards that allow users to trade some voice quality for bandwidth by selecting a different compression standard (G.711 or G.723). Consequently, packet loss and delay are crucial to the Quality of Service.

Packet Loss

Packet loss can occur for reasons discussed in Bandwidth, Congestion, and Connections, next.

Bandwidth

Bandwidth is the capacity to carry information. By using H.323, the same bandwidth that supports one uncompressed G.711 voice connection can, instead, support several compressed G.723 conversations with little noticeable difference in quality.

Networks differ in the age of their equipment and in the quality of their service. Traffic can form a bottleneck if network loads force a wide area service provider to route traffic through old equipment.

Congestion

Users notice congestion when audio "breaks up" during a call. Congestion can occur anywhere on the network, for example, at an overloaded LAN (local or remote), at an overloaded router or firewall, or within an overloaded internet. Because voice packets are only significant during a conversation, IP networks respond to congestion by discarding data packets they cannot accommodate. Resending or delaying packets is not an effective solution.

At the local level, congestion symptoms can be subtle. For example, routers from different vendors can respond differently to congestion because of the way they prioritize their response to packet congestion.

When considering communications problems, it is important to maintain reserve capacity and to use a systematic approach that considers the entire, end-to-end, connection.

You can reduce NBX system's bandwidth requirements by enabling "silence suppression," but doing so compromises audio quality. 3Com telephones generate voice frames at regular intervals for the duration of a connection. These frames normally continue when no one is speaking. When you enable silence suppression, the system sends a "silence indicator" when the telephone senses the start of a silent period. When another device receives this indicator, it inserts "white noise" until it receives the next frame that contains real voice. All subsequent "voiceless" frames are suppressed during the silent period. However, most telephone users will notice the difference between genuine silence and generated silence.

This type of silence suppression applies to Layer 2 Ethernet transfers. At Layer 3, the ConneXtions software achieves a similar result by not sending empty packets during a silent period. The receiving ConneXtions gateway generates a silence indicator or sends frames filled with silence, depending on the silence suppression mode.

Connections

Sometimes packet loss is caused by a poor physical connection. This type of packet loss is more likely to occur in a LAN than in a WAN. Typical

causes are faulty wiring, connectors, and termination. High-bandwidth LANs (100BASE-T) are more likely to have termination problems than 10BASE-T LANs.

Packet Delay

Latency and jitter delays affect the Quality of Service.

Latency

Latency is the sum of all the fixed delays in an end-to-end connection. Latency prevents a caller from responding immediately to another caller's remarks.

Most people notice latency when the end-to-end delay is above 200 ms. (The round-trip delay is typically no greater than 400 ms.) Conversations sound most natural when latency is below this range. Network latency can be measured by "pinging" the network connection, but the network connection is only part of the delay. The entire end-to-end delay also includes the H.323 gateway, firewall or router, and the LAN itself. System administrators can control some local device delays by controlling the system load and by upgrading system components as needed.

Jitter

Momentary transmission delays can affect the pace of a conversation and, if severe, cause the voice to "break up." This is known as "jitter."

All voice-over-internet devices have a "jitter buffer" at the receiving end whose purpose is to absorb jitter. It does this by delaying the first packets that arrive by some significant amount (from 50 to 200 ms). This delay creates a window of time for receiving the next group of related samples which are then forwarded to a callee at a regular rate. However, if some packets are too late, and exceed the jitter buffer capacity, those packets are lost and there are gaps in the audio.

Quality of Service Control

NBX systems address Quality of Service (QoS) issues using methods that are discussed in this section.

Adaptive Jitter Buffering

All IP network devices use buffers to retime the packets that they receive from a network. Retiming allows these devices to compensate for the variable delays that occur as the packets pass through an IP network. H.323 calls take different paths through a network so the ConneXtions

gateway uses an adaptive "jitter buffer" to minimize delay variability. Initially, the jitter buffer delays the entire packet stream by 50 ms, an amount that is too small to be noticed in conversation, but large enough to account for the variability.

If the packet delays are too variable, packets might not arrive in time to be useful. This can result in lost packets and gaps in the conversation. When ConneXtions detects the gaps caused by late-arriving packets, it automatically extends the jitter buffer delay to match the delay so similar packets are not lost. ConneXtions can extend the jitter buffer delay up to its 200 ms limit.

Reconstruction

3Com Business and Basic Telephones expect to receive voice packets at regular intervals, but unanticipated network delays can cause lost packets and gaps in the conversation. Reconstruction makes these gaps less noticeable with "best guess" substitutes based on the preceding and following samples.

If your network is not optimized for voice, the quality of voice can be affected.

Priority Schemes

Packet-based voice systems depend on the speedy and consistent delivery of voice packets for good voice quality. This dependency presents an obstacle to H.323 communication on the Internet because it was designed to treat all packets alike with respect to time. By treating packets that carry e-mail with the same priority as packets that carry real-time voice, the Internet ignores the important differences between these applications.

NBX systems use the latest developments to address voice packet priority concerns at the Layer 2 Ethernet level and at the Layer 3 IP network level.

Layer 2 NBX systems address Layer 2 priority concerns through the 802.1(p and q) standards. These standards have two parts. The first part addresses the way Ethernet frames get onto the local "wire." The system uses a special "back-off" algorithm that gives voice frames a higher priority when both voice frames and data frames try to access the Ethernet wire at the same time.

The second part of the 802.1(p and q) standards addresses the way LAN switches prioritize different packets that are competing to enter a different LAN segment. This scheme is based on a 3-bit priority field within the Ethernet header.

*NBX ConneXtions does not support the Layer 2 (Ethernet) 802.1 (*p and q*) priority field. However, it is usually possible for IP routers to use these priority schemes if they are configured to prioritize H.323 packets.*

Layer 3 NBX systems address Layer 3 priority concerns through a packet priority scheme called "IP/DS" (for differentiated services). Many routers support this scheme, which replaces an earlier scheme (TOS), which uses a 6-bit priority field within the IP header of every packet. Most routers examine this field and base their pass-through priorities on it.

NBX systems are designed to use the default values that come with 3Com switches. If you use other routers, you might need to reprogram their diff-serv settings. The 3Com default is 101110xx. This setting must be consistent at both ends of the connection. Note that some routers overwrite the TOS field (diff-serv priority field) and eliminate the priority distinctions between packets.

NBX ConneXtions does not support the Layer 3 (IP) 6-bit TOS/DS priority field. However, it is usually possible for IP routers to use these priority schemes if they are configured to prioritize H.323 packets.

Special Issues

This section describes issues related to H.323 telephony in general and to ConneXtions gateways in particular. These include:

- Firewall Security
- Gateway Load
- Remote Access
- PBX Connections
- Class of Service
- IP Type of Service and Differentiated Services
- Alternate Gatekeepers

Firewall Security

Firewalls determine which packets can cross the boundary between a protected network (intranet) and the public internet. The network

administrator specifies crossing privileges according to network needs and policies. Control criteria consists of direction of transfer, source and destination address, packet type, and access ports.

Firewalls affect, and are affected by, H.323 gateways. For example, firewall processing increases packet delay while the complexity of the H.323 protocol complicates the firewall programming.

The only way to safely avoid firewall delays is to exclude outside internet access. This means calls can only be made within the secure intranet.

In some business applications, it is possible to eliminate the firewall delay by setting up a dedicated physical connection between the H.323 gateway and the router. This approach, which requires a second NIC in the ConneXtions PC system, bypasses the firewall and puts the burden of discriminating against non-H.323 packets on the gateway. The PC system that runs the ConneXtions software must be secure.

Systems that must conform to very conservative firewall policies can use a Virtual Private Network (VPN) if they need to filter incoming H.323 calls from the public Internet. An alternative is to use a firewall with H.323 proxy support.

While the operating system that runs the H.323 gateway can be programmed to serve both as an H.323 gateway and as an IP router, such arrangements are usually impractical because the gateway needs so much processing power just to manage audio conversions.

3Com recommends that a high-performance PC be dedicated to the ConneXtions software.

The question of whether an operating system is adequately "secure" is a subject of debate. The concern is that Windows has many IP ports of its own. One way to deal with these ports is to set up a firewall that limits the range of externally accessible ports. However, some organizations connect the ConneXtions gateway directly to the Internet through a second NIC that bypasses the firewall protecting the rest of the local network. ConneXtions supports either configuration.

Organizations that want to completely bypass firewall delays can research the large volume of security information about the subject.

These descriptions focus on the firewall-protected approach, and offer guidelines for programming a firewall that can be used to support H.323 connections that are accessible to the public internet.

Outbound Calls

Most firewalls do not restrict outbound packets or IP packets that respond to outbound initiatives. They are configured for unrestricted outbound packets with unrestricted reply packets. They do not have to be changed to support outbound H.323 calls from a system.

Inbound Calls

Firewalls usually discriminate against incoming packets. The network administrator configures a list of acceptable sources for each destination address within a protected network. The configuration list includes a list of entries that the firewall compares to the IP address of the local H.323 gateway and the IP address of an external caller. The configuration list also discriminates for or against specific types of packets. IP addresses and packet types must match for packets to pass.

The H.323 protocol uses TCP packets for call setup, and UDP packets to carry the voice payload. Each type of packet includes an array of port addresses that are used during the connection. Ports 1720 negotiates which of the other available ports is used to carry the connection.

The ConneXtions gateway uses these default port assignments:

- For UDP traffic, ConneXtions uses ports 8000-8099 by default. Calls require four UDP ports each.
- ConneXtions uses ports 1025-5000 for TCP traffic. You can configure TCP ports during installation.

During ConneXtions installation, you can configure the TCP ports that are used for incoming calls. For outgoing calls, no control is possible. Port 1720 must be preserved.

You must configure a firewall to accommodate both TCP and UDP ports on the same system.

Gateway Load

If the gateway system NIC is attached to a LAN with heavy packet traffic (more than 700 non-H.323 packets per second), the extra address processing burden, which requires processing power, can slow down the

gateway. This occurs because the ConneXtions software makes H.323 ports look like hardware line cards to a Call Processor.

To emulate a group of simulated line cards, the gateway system must read the destination address of every frame that is presented to its Network Interface Card, instead of responding to only one hard-coded Ethernet address. The gateway system is able to examine every Ethernet frame because its NIC does not discriminate between frames. The NIC passes every frame that it sees to the software for address evaluation.

To reduce the load on an H.323 gateway, you can connect it to an existing multi-port switch. For optimum performance, use switches that support 802.1(p and q). The 802.1(p and q) standard offers priority enhancement which NBX systems exploit. Most 3Com switches support this feature.

Remote Access

Business people who travel can make routine calls without long distance line charges by using an internet-ready laptop with Microsoft NetMeeting to make H.323 calls, and a Virtual Private Network (VPN) connection to the NBX system LAN. Microsoft NetMeeting software works with Windows 2000 and it can be downloaded for free from *www.microsoft.com.*

You can use Microsoft's VPN Dial Up Networking (version 1.3) to establish a virtual private network connection between a roaming laptop and the NBX system LAN. One end of the VPN connection is in the laptop while the other end must be located in a VPN server between the router and firewall.

The VPN server provides caller authentication and a secure (encrypted) channel across the internet. After a caller has been authenticated, the connection is passed to the firewall, which sees the VPN connection as coming from a recognizable (and therefore firewall-configurable) IP address. VPN allows a business person to establish an IP connection into the NBX LAN from a hotel room with internet service.

After an Internet connection has been established, change your automatic call forwarding number:

1. Log on to NetSet as a user.
2. On the *User Information* tab, click *Call Forward*.
3. Click the telephone number radio button.

4 Enter the number to which you want to forward the call and click *OK*.

The caller is now ready to use NetMeeting to place an H.323 to the system at the office. Configure NetMeeting with the IP address of the ConneXtions gateway as the gateway in Advanced Calling options. Dial the extension to place the call.

The call passes through the Auto Attendant to your extension and forwards the call to your previously specified number.

After the call, return to NetSet and remove the forwarded number so that work-related calls to your extension are not forwarded to your home, or to wherever you placed your last H.323 call.

PBX Connections

H.323 gateways allow NBX systems to establish IP connections to other H.323-equipped PBX systems as well as to similarly equipped NBX systems. Although H.323 standards describe a universally accepted interface for interconnecting similar systems, each of the 20 or 30 PBX manufacturers brings its own PBX solution to the marketplace. The diversity of products and release levels that are associated with each manufacturer increase this complexity further. Because any implementation differences can affect connectivity, this manual can only offer guidelines for connecting NBX and PBX systems.

Tie-line connections between NBX and PBX systems require technical people from both ends of the connection to collaborate in these major areas, discussed next:

- H.323 Interoperability
- IP Addressing
- Voice Ports
- Extension Dial Plans
- Extension Delay

H.323 Interoperability

H.323 protocol stacks provide the foundation for H.323 compatibility. Each consists of a collection of engineered software products that implements the H.323 standard. Although PBX manufacturers can develop their own H.323 software stacks, it is more efficient to purchase software licenses from a company that specializes in developing H.323 protocol stacks.

The ConneXtions gateway has been tested for compatibility with PBX H.323 gateways that are licensed to use Lucent Elemedia and RADVision H.323 protocol stacks. It has also been tested with these H.323 telephones:

- Siemens HiNet LP 5100 (phone application version 1.1.3)
- ACT Sagitta PH200
- Microsoft NetMeeting (version 3.0)

IP Addressing

The main goal of an H.323 gateway is to provide telephone-like service through IP connections. This means each end-to-end connection involves two types of addresses: a normal telephone number (E.164 address) and an intermediate IP address. Some H.323 implementations use a "gatekeeper" to convert the E.164 number into the appropriate IP address at the calling side, and then to reconvert the IP address to the E.164 number at the receiving side (for caller ID purposes). ConneXtions allows you to choose if you want to use a gatekeeper on your network.

Outgoing IP addresses can be entered:

- As pre-programmed speed dial numbers that forward callers to the Auto Attendant at a remote NBX system.
- By modifying the dial plan.

You can configure the speed dial numbers to include an appended extension if a person in one NBX system needs to make frequent calls to someone in another NBX system. Alternatively, you can configure the dial plan to route these calls seamlessly to the caller.

NBX system calls to outside numbers must use IP addresses or host names. The ConneXtions software automatically converts host names to their corresponding IP address.

Voice Ports

Multiple voice ports allow the Auto Attendant to respond to multiple incoming calls at the same time. However, since these ports are also used by the voice mail system, voice mail inquiries can slow down incoming H.323 calls. You might have to increase the number of voice port licenses.

Extension Dial Plans

PBX systems can use different dial plans. You must consider dial plan differences when setting up calls between systems. Dial plans differ in their use of leading digits, number of digits, and excluded numbers. For more information, see Chapter 11.

Extension Delay

Call setup times for digital connections, compared to analog connections, are instantaneous so there is no need to include a delay between the IP address and an appended extension.

Incoming H.323 calls to a system usually go directly to the Automated Attendant. Although the Auto Attendant can respond with voice instructions, the call does not have to wait until the end of the voice instruction to respond. The Auto Attendant accepts extensions whether they are entered manually or as part of a speed dial number.

Class of Service

The use of an H.323 gateway affects the Class of Service assignments that are applied to extensions because:

- H.323 calls use IP addresses instead of the familiar numbers that are used for public switched network calls (different dial plan).
- The cost of an H.323 call is distance-independent, so you do not need to limit long distance calling for cost reasons.

External Call Control

Users of ConneXtions-equipped systems can place H.323 calls to other H.323 systems anywhere in the world without having to pay long distance charges. Since there are no long distance charges for H.323 calls, there is no need to restrict them for cost reasons.

IP Type of Service and Differentiated Services

The header of each IP packet contains an 8-bit Type of Service (TOS) field that indicates the precedence (relative importance) of the packet. Routers then examine the TOS field and give precedence to packets with a higher TOS setting.

Although your telephone system supports prioritization using the TOS field, this facility is not supported for H.323 calls. However, for H.323 calls over the WAN, routers can prioritize voice traffic using alternative means. For example, during installation, you can select a range of UDP or TCP port addresses to help with router setup.

Alternate Gatekeepers

A zone can contain only one gatekeeper at a time, although multiple distinct devices can provide the gatekeeper function in a zone. Multiple devices that provide the RAS signaling function for the gatekeeper are called alternate gatekeepers. Each alternate gatekeeper appears to each endpoint as a distinct Gatekeeper.

To ensure system availability, redundancy, and scalability, the gatekeeper can provide RAS signaling function by using multiple physical or logical devices, referred to as alternate gatekeepers.

Checking Connections

You can use connection checks to pre-qualify an installation and to localize connection problems. H.323 gateway installers can conduct connection checks for:

- Gateway Checks
- Network Checks

Gateway Checks

Gateway checks can verify that the systems at each end of an H.323 connection are working properly.

Gateway Self-Check

A gateway self-check is simply an H.323 call that returns to the local IP address (loopback test).

To perform a gateway loopback test:

1. Access a ConneXtions H.323 port from an 3Com Business or Basic Telephone by dialing an H.323 port line number or by using a dial plan configured with a ConneXtions pool number.

You must have Super User Group CoS allowed to dial in to a line port number directly.

2. Enter the IP address of the gateway.
3. Verify the connection. If you are using default settings, you are connected to the Auto Attendant. If you are not using default settings, you might be connected to a different extension number.

Local Considerations

All voice packets that move between an 3Com Business or Basic Telephone, Call Processor, ConneXtions gateway, and router on the LAN have a high priority and high quality of service.

However, at the router and beyond, network administrators can influence H.323 call quality through the priority that they give to H.323 packets at both the internet router and at the firewall.If H.323 connections consistently experience significant delays, review the local router and firewall configurations at each side of the H.323 connection.

Network Checks

A network check uses:

- Network Ping
- NetMeeting Connections

Network Ping

A network *ping* is a packet transfer that checks the logical continuity between a personal computer and a specified IP (router) address. For example, you can ping your own address, or the default gateway. The next ping checks the connection to the IP router at the remote end of the intended H.323 connection.

The easiest way to initiate a ping is with a DOS ping command. This command sends four pings to the specified IP address. The router at that address immediately returns the ping, and the command notes the round trip delay for each ping packet. Some firewalls do not return pings for security reasons. If the ping test fails, you can use a "trace router" command ("tracert") to find out where the logical connection failed.

To check a connection:

1. Access the DOS command prompt from the DOS shell in Windows.
2. Enter `ping` on the command line:

   `ping <192.168.1.190>` (sample IP address)
3. Interpret ping results:
   - **a** `Request timed out` (all four times)
     - Ping reached the network but couldn't connect to the host
     - (No such address; or the device is down.)
     - Initial request timed-out
     - (It is normal for a first ping to fail and subsequent pings to succeed.)
     - Subsequent requests timed-out

- (Indicates some packet loss. Rerun using the "-n 100" option. The "request timed out" number represents the percentage of lost packets. These packets could have been lost in either direction.)

b `Destination host not reachable`

- Ping couldn't negotiate a path to the specified address

  (PC is not plugged into LAN, incorrect gateway address in route, or a firewall blocked the ping.)

c `Approximate round-trip times in milliseconds`

- Ping time greater than `10 ms` but preferably less than 300 ms.

  (Ping times can differ because the network often routes individual packets along different internal routes depending on congestion.)

4 Use `tracert` on the command line:

`tracert <192.168.1.190>` (example IP address)

5 Interpret trace results:

The `tracert` command lists every IP gateway it encounters as it tries to reach the specified destination. It also includes the number of times (3) required to reach each intermediate gateway. If a network connection failure occurred in route, this command indicates where it occurred.

Because the `tracert` command reveals the chain of logical connections across a network, it can be useful for comparing the performance of alternative internet service providers.

NetMeeting Connections

You can also check H.323 voice packets that are sent between systems that are running Microsoft NetMeeting. ConneXtions software requires it to run G.711 (CCITT mu-law) or G.723.1 compression. NetMeeting is available on the Resource Pack CD, or it is available as a free download from `www.microsoft.com`.

You can conduct the NetMeeting connect test from the operating system that runs the ConneXtions software, or from another PC on the LAN.

You must run NetMeeting and ConneXtions on different PCs.

In addition to the NetMeeting software, participating computers need an audio card with a headset (or speakers) and a microphone. The audio card must support full-duplex 64 Kbps transfers.

Note that it is possible for a NetMeeting connection to be unsuccessful and still have a successful ConneXtions installation. This can occur because ConneXtions restricts the range of TCP and UDP ports used but NetMeeting allocates its ports from a wider pool. For more information, see "Firewall Security" on page 480. If ConneXtions is installed with a limited range of allowable ports, and the firewall is configured to pass only those ports, it is possible that NetMeeting cannot pass a call through the firewall while the more restricted ConneXtions calls can pass through.

The following procedure uses NetMeeting to test the connection between the operating system that runs the NBX ConneXtions H.323 Gateway and a remote IP address. This end-to-end NetMeeting check can help to recognize firewall problems without the complexity of the system and ConneXtions H.323 server.

To make a NetMeeting check:

1. From the *Start* menu, select *Settings*, and then *Control Panel*.
2. Select *Applications* and then *Services*.
3. Select *3ComConnextions* from the list, and click *Stop.*
4. Access `www.microsoft.com` using a web browser.
   a. Click *Downloads* in the navigation bar.
   b. In the *Product Name* field, select *NetMeeting*.
   c. In the *Operating System* field, select *Windows 2000*.
   d. Click *Find It!* The latest versions of NetMeeting are displayed. Click the version you require.
5. Download NetMeeting files and respond to the prompts.
   a. Click the program name (`NM30.exe`) next to *Download Now.*
   b. Click *OK*.
   c. In the *Save As* dialog box, select a folder for the downloaded files.
   d. Click *Save.*
6. Install the NetMeeting files and respond to the prompts:
   a. Select *Open* when the download is complete.
   b. Click *Yes* to confirm installation.
   c. Click *Yes* to acknowledge the legal agreement.
   d. Click *OK* to accept the default installation directory.

e Click *OK* to acknowledge successful installation.

7 Open NetMeeting:

a Click *Next* on next two windows.

b Enter your details as required.

c Click *Next* on next two windows.

d Click *Put a Shortcut to NetMeeting on My Desktop.*

e Click *Next* in next two windows.

f Click *Test.*

g Adjust the speaker volume.

h Click *Next.*

i Click *Test.*

j Adjust the microphone Record Volume.

k Click *Next.*

l Click *Finish.*

8 To attempt a NetMeeting call:

a Click the NetMeeting icon, followed by the telephone icon.

b Enter the IP address of similar system at remote end, after *To*.

c Select *Network* or *Direct Call*, after *using*.

d Click *Call.*

e Confirm the connection using a speaker or headset and microphone.

9 To end the call, click the "hang-up" icon.

Interpreting the Results

The NetMeeting check has three possible outcomes:

- No communication with remote NetMeeting.
  Wrong IP address.
  Firewall is blocking call setup (TCP) packets.
- Call rings remote end and it answers, but there is no audio.
  Faulty connection to a microphone, speaker or both.
  Firewall is blocking audio (UDP) packets.

- Calls work in one direction, but not in the reverse direction. Place a call to determine which firewall is blocking TCP traffic. Once you determine this, it is the *remote* firewall that is blocking the traffic.

Placing Calls

You can place an outgoing H.323 call from a system in one of several ways, as discussed in this section.

See Chapter 11 for information about how to use the dial plan to set up the system to use H.323 ports.

IP Address Entry

Depending on how you set up the dial plan, the most convenient way to place a call to a new number is to dial a ConneXtions extension list (configured within the dial plan), which provides a connection to an available H.323 port. If a port is available (not busy), enter the extension and IP address from the telephone key pad. Use the * key to separate the four "octets" in the IP address, and then press the # key to "dial now."

You must configure the dial plan to use ConneXtions. You must have Super User Group CoS privileges to perform this test.

These examples show key pad sequences that request an extension list connection and a specific port connection:

8192*168*1*15#

where extension list access is used

OR

754 192*168*1*15#

if there is no extension list access, or if you want to test specific ports.

The first example begins with an 8 to request any available H.323 port. The second example begins with the 3-digit extension (754) of a specific H.323 port. The remaining digits in both examples represent the IP address of the remote H.323 gateway (192.168.1.15). Note that IP addresses are always four octets long. In this case, 15 is the last octet.

Extension Lists

You can configure H.323 ports for single-digit access (usually 8) instead of a specific 3-digit line extension. The single-digit access allows the system to select an available line port when you place an external call.

Internet IP line ports and CO (central office) line ports must never be assigned to the same extension list because they use very different dial plans. Conventional practice is to use 9 for external switched network (PSTN) connections and 8 for external IP network connections.

Calls to other NBX systems (or PBX systems) can include a destination extension. This example represents a call to an extension (273) on a remote NBX system that has an H.323 ConneXtions gateway:

8192*168*1*15*273#

The # sign tells ConneXtions to "dial now." The last asterisk, *, terminates the IP address, but ConneXtions cannot dial the number until it sees the "# sign," or until 4 seconds pass after the last digit. In the preceding example, the IP address (192.168.1.15) and the extension are presented to the device as the "called party."

The # sign also precedes the extension as shown below. This allows the ConneXtions gateway to complete the IP connection before it presents the remaining digits to the remote terminal:

8192*168*1*15#273

Both configurations produce the same result when dialing into another NBX system; however, other PBX systems can be position-sensitive. If you are not sure, use the first format with the # sign after the extension.

Speed Dials

Your telephone system has a speed dial capability that offers a quick way to dial frequently called numbers. Each telephone is capable of accessing 199 previously stored dial sequences with up to 30 characters in each sequence. These sequences can represent switched network numbers or Internet addresses. Special 3-digit speed dial numbers specify each dial sequence.

Speed dial numbers must be preceded by the "Feature" button when entered from a telephone. This button distinguishes speed dial numbers from ordinary extensions that use the same three digits.

Speed dial numbers can be system-wide or personal. System speed dial numbers (700-799) apply system-wide and are programmed by the system administrator. Personal speed dial numbers (601 through 699) apply only to an individual telephone; they are programmed by its owner.

You can assign any of the first ten speed dial numbers in each type group, system or personal, to any Access button on a telephone. For more information, see Chapter 6 of the *NBX Telephone Guide*.

Setting Up Speed Dials

The following procedure assumes that you are logged on to NetSet as an administrator, and that you know the H.323 port extensions that were established during installation.

To set up speed dials:

1. Click *PSTN Gateway Configuration* > *Analog Line Cards*.
2. Note the extension number of each listed H.323 port.
3. Click *Feature Settings* > *System Speed Dials* tab.
4. To complete the fields:
   a. Note a speed dial number. (One-button dialing requires system speed dial numbers 700 through 709.
   b. In the *New Number* field, type an H.323 extension, or an 8 (for extension list), followed by an IP address, or a system name. Examples are:

      8192*168*1*15*273# (IP address plus extension)

      8192.168.1.15*273# (IP address plus extension)

      8273@h323.nbx.com# (extension plus host name)

      8h323.nbx.com# (host name, defaults to AA)

      Use those characters shown here, that is, no spaces, hyphens or & signs.

   c. In the *Comment* field, enter a description with up to 30 characters, such as *Tie-line to NYC,* and then click *Apply.*
5. Verify the speed dial entry by pressing the *Feature* button followed by the new speed dial number.

One Button Access

You can configure an Access button on a system to dial a complete H.323 (or switched) dial sequence.

This procedure assumes that all buttons available for one-button access are configured in the first ten system (or personal) speed dial locations.

To set up one-button dials:

1. Click *Telephone Configuration*.
2. Click the *Telephones* tab or the *Group Telephones* tab. Select a telephone extension or a telephone group.
3. Click *Button Mappings.*
4. Associate one of the first ten speed dial numbers with a telephone Access button:
   - **a** Locate the *Type* field associated with an available button.
   - **b** Select the speed dial selection (SSD 0 through 9) that is associated with a previously programmed speed dial code (700 through 709).
   - **c** Click *Apply* and then click *OK* (to return).
5. Verify the one-button dial feature operation by pressing the new button and confirming that it dials the specified number.

Entering Digits During Calls

When ConneXtions dials a call, it stores the dialed digits until it connects the call. Then it sends those digits, and any subsequent digits, to the remote H.323 device if the device supports version 2, or later, of the H.323 standard.

The behavior of ConneXtions depends on when the # sign is entered during this process.

ConneXtions sends digits as messages, which are more reliable than audio tones. ConneXtions also expects to receive digits from H.323 devices in the same way, and therefore does not have a tone detector. This means older (H.323 version 1) devices cannot send or receive digits to or from ConneXtions. For example, the current version of Microsoft NetMeeting, which sends DTMF tones in the audio stream (in-band signaling), cannot use DTMF signaling to pass the Auto Attendant.

In instances where other devices might listen for in-band DTMF signaling, the quality of the tone recognition depends on the selected voice compression. Tones transmitted by G.711 can be reproduced, but tones transmitted by G.723.1 are degraded.

Receiving Calls

ConneXtions gateways route incoming calls to any available H.323 port. The system then connects this port to the extension specified during port

configuration. H.323 ports are configured through the system software just like line card ports. Selectable extensions are:

- Auto Attendant (500)
- Receptionist's telephone (usually the lowest numbered extension on the system. Default:
  - V3000, V3001R, and V5000 systems: 1000
  - NBX 100 system: 100
- Other extensions (each ConneXtions H.323 port can go to a single extension)

Auto Attendant

H.323 calls are usually routed to the Auto Attendant. From there, callers can reach internal extensions without operator assistance by supplying a 3-digit extension when setting up the call (as the called party), or by dialing an extension after the Auto Attendant answers. Callers cannot get an outside line through the Auto Attendant because dialing 9 normally diverts incoming calls to the name directory.

You can configure H.323 calls to appear to go directly to an internal extension by adding a 3-digit extension immediately after the last octet in an H.323 IP address. Do not use commas, spaces, or hyphens between the IP address and an extension when programming an H.323 speed dial number. IP network connections do not incur delays like those that occur with analog PSTN connections.

8192*168*1*15*273#

The # sign in this example indicates when the last digit was entered so that the Call Processor does not have to wait 4 seconds to determine that a caller has no other digits to dial.

Caller ID Response

The Auto Attendant receives caller ID information from an outside caller and passes it to a caller-selected extension. On a telephone, the caller ID name and extension (if applicable) appear in brackets to indicate that the network has not authenticated the enclosed information.

Attendant Console

By convention, systems reserve extension 100 or 1000 for the Attendant Console (receptionist), although the Attendant Console can be assigned any internal extension number. Outside callers cannot reach internal extensions without operator involvement when incoming calls

are directed to the Attendant Console. See "Adding an Auto Attendant" in Chapter 9.

Other Extensions

Incoming H.323 calls can be routed directly to some other extension or to a phantom mailbox. Sales people often have phantom mailboxes because they are never in the office. Calls to their extension go directly to their voice mailbox. Note that phantom mailbox extensions cannot be used to forward calls.

Setting Up an H.323 Port Route

After you install an H.323 line port, you need to configure it.

To configure a H.323 line port:

1. Click *PSTN Gateway Configuration*.
2. Click *Analog Line Cards*.
3. Select an H.323 port. This port has the default setting from the Auto Discovery installation process.
4. Click *Modify*.
5. In the *AutoExt* field, enter the required extension number.

CAUTION: *Do not route an H.323 port directly to another line port. Routing an H.323 call to a PSTN line, from the Internet, is dangerous because it would allow anyone to make long distance toll calls through the Call Processor — with no accountability.*

6. Click *OK*.

Handling Conference Calls

You can include gateway port connections in local conference calls along with PSTN line connections. However, ConneXtions does not support conferences at the H.323 level, so, if two or more of the conferring parties are at a remote system, each requires a separate port connection. This characteristic determines who can initiate the conference call.

A four-way conference call with three people at one site and one person at the other site uses one H.323 port if it is set up from the side with three people. Otherwise, it needs three ports.

Related H.323 Documentation

Here are some useful sources of information about the H.323 standard:

Web Sites

- http://www.packetizer.com/iptel/h323/
- http://www.itu.int/itudoc/itu-t/rec/h/

Book

IP Telephony: Packet-Based Multimedia Communications Systems — Olivier Hersent, David Gurle, Jean-Pierre Petit (1999).

E CALLER ID

Caller ID behavior varies depending on the type of device and the conditions under which the call is received. This appendix describes these caller ID conditions:

- Forwarded Calls and Caller ID
- Long Caller ID Character Strings
- Specific Caller ID Situations

Forwarded Calls and Caller ID

While a *forwarded* call is ringing on a telephone:

- On the top line in the telephone's display panel, the Caller ID of the original caller displays and a greater than (>) character on the left side of the display helps you to visually identify the Caller ID of the original caller.
- On the bottom display panel line, the Caller ID of the telephone that is performing the transfer displays.

After the call is answered, only the Caller ID of the original caller remains in the display and the greater than (>) character is removed.

Long Caller ID Character Strings

Some models of the 3Com Business Telephone can display two lines of 16 characters while other models of the 3Com Business Telephone can display two lines of 24 characters. The displays of different brands and models of analog telephones with built-in Caller ID can show either 16 or 24 characters per line. The same is true of Caller ID boxes that are connected in-line with analog telephones.

If the length of the Caller ID information on either the top or bottom line exceeds the width of the telephone display panel, the information is truncated for the first five seconds. After five seconds, the Caller ID information on the bottom line is cleared, and any truncated information

from the top line displays on the bottom line. After an additional five seconds, if the Caller ID information from the top line exceeds the capacity of both display lines, the numeric portion is removed and only the name portion displays in the display.

Specific Caller ID Situations

The Caller ID information that the telephone display panel displays can be different in some specific call situations.

Analog Telephones

Analog telephones can use these interfaces to connect to the system:

- Single port Analog Terminal Adapter
- A port on an Analog Terminal Card
- Citel Analog Interface Card

Analog Terminal Adapter and Analog Terminal Card Ports

If you have an analog telephone connected to the system using a single port Analog Terminal Adapter or to a port on an Analog Terminal Card, the behavior of Caller ID on the analog telephone (or on Caller ID boxes connected in-line with the analog telephone) depends on whether the Caller ID device/telephone supports 2-line Caller ID display.

- Most analog telephones with built-in Caller ID and most Caller ID boxes do not support 2-line display of Caller ID information. For this type of device, only the Caller ID of the original caller displays.
- If the analog telephone or Caller ID box supports 2-line display of Caller ID information, the information displays in the same way as it does on an 3Com telephone.

If the Caller ID information exceeds the capacity of the Caller ID display (some can display 16 characters and others can display 24 characters) the Caller ID information is typically truncated at the width of the display.

Citel Analog Interface Card

If you have analog telephones connected to the system using the Citel analog interface card, the behavior of Caller ID on the analog telephones is the same as the behavior of analog telephones connected to a single port Analog Terminal Adapter or a port on an Analog Terminal Card. See "Analog Terminal Adapter and Analog Terminal Card Ports" on page 500.

Bridged Extension Telephones

Caller ID information displays in exactly the same way on a bridged extension telephone as it does on a non-bridged extension telephone. See "Caller ID" on page 499 and "Long Caller ID Character Strings" on page 499.

Calls That Are Forwarded Multiple Times

If a call is forwarded several times, the Caller ID information of the original caller displays on the top line of the display panel of the ringing telephone and the Caller ID of the telephone that most recently forwarded the call displays on the bottom line. A greater than (>) character displays to the left of the original Caller ID on the top line in the telephone display panel.

Example: A places a call to B, who answers the call and forwards it to C, whose telephone is forwarded to D. While telephone D is ringing, the top line in the display panel contains the Caller ID for A and the bottom line contains the Caller ID for C. After 5 seconds, only the Caller ID information for A displays.

External Calls

The display of Caller ID information for external calls depends on how the call arrives at the system.

External Analog Line Card Calls

An external call arrives at a system on an Analog Line Card port and is routed to A's telephone.

When A transfers the call to B, the Caller ID (if any is provided by the telephone company) displays in the top line of B's telephone display panel. If no Caller ID information is available, the extension associated with the Analog Line Card port displays on the top line. A's Caller ID information displays in the bottom line.

Exception: An Analog Line Card port is mapped to an internal extension.

The call is not answered and goes to the call coverage point for the extension. If the coverage point is the receptionist's telephone, for example, the receptionist sees the Caller ID information only for the external call, and not for any telephone on which the mapped Analog Line Card Port displays.

External ISDN BRI Calls

An external call arrives at a system on an ISDN BRI channel and is routed to A's telephone.

When A transfers the call to B, the Caller ID (if any is provided by the telephone company) displays for five seconds in the top line of B's telephone display panel. If no caller ID information is available, the Trunk name and channel number from the Digital Line Card appear on the top line of B's telephone display panel. A's ID displays on the bottom line.

External ISDN PRI Calls

An external call arrives at a system on an ISDN PRI channel and is routed to A's telephone.

When A transfers the call to B, the Caller ID (if any is provided by the telephone company) displays for five seconds in the top line of B's telephone display panel. If no caller ID information is available, the Trunk name and channel number from the Digital Line Card appear on the top line of B's telephone display panel. A's ID displays on the bottom line.

External T1 Calls

An external call arrives at a system on a T1 channel and is routed to telephone A. If the call is transferred to B, the display of caller ID information on B's telephone depends on which *Incoming Call Digit Format* is configured on the T1 board.

- **DNIS/DID** — The T1 board is configured to expect either Dialed Number Identification System digits or Direct Inward Dialing digits.

  If DNIS digits arrive, there is no Caller ID information. Instead, the system displays the name of the T1 trunk and the extension associated with the T1 channel.

- **DNISANI** — The T1 board is configured to expect Dialed Number Identification System digits followed by Automatic Number Identification digits.

  The system displays the ANI portion of the incoming digit sequence followed by the name of the T1 trunk and the extension associate with the T1 channel. The ANI field can be configured to capture either 7 or 10 digits of ANI information.

Internal Calls On a single system, user A calls B who transfers the call to user C. In C's telephone display panel, the top line contains Caller ID information for A and the bottom line contains Caller ID information for B.

Nortel Phones If you have Nortel telephones connected to your system using the Nortel interface card, the behavior of Caller ID on these telephones is identical to the behavior on 3Com telephones.

Parked Calls When you retrieve a parked call, the Caller ID associated with the call displays for approximately five seconds in your telephone display panel. You do not see the Caller ID of the person who parked the call.

Second Incoming Call If you are currently involved in a call on your telephone and another call arrives, for approximately five seconds you see "Incoming Call" on the top line of the telephone display panel and the Caller ID of the incoming call displays on the bottom line.

TAPI Calls If a call is forwarded to a telephone that is controlled by TAPI software, both the original Caller ID and the Caller ID of the person forwarding the call are sent to the TAPI software.

TAPI Redirected Calls If telephone A is being monitored by an external TAPI application and a forwarded call to A is redirected to telephone B, the TAPI software passes the Caller ID of the original caller and the Caller ID of the forwarding telephone to telephone B.

VTL Calls If A1 calls A2 who then forwards the call to B1 over a Virtual Tie Line connection, the Caller ID information for A2 displays in the display panel on B1's telephone. The Caller ID information includes the IP address of System A and the extension number of A2.

See "Adding VTL Devices to the Pretranslators (Optional)" on page 338 for information about how to remove the IP address from the Caller ID information or change it to the VTL site code for that site.

Calls Transferred to Hunt Groups When someone performs a blind transfer to a hunt group, telephones in the hunt group display the called ID information of the original caller on line 1 and the hunt group name and number on line 2. After a hunt group member answers the call, only the caller ID information of the original caller displays.

3Com Cordless Calls The 3Com Cordless handset shows DTMF entries that briefly start from the bottom right hand corner of the display, then shift to standard screen placement. This behavior is normal for this telephone.

F OUTBOUND CALLER ID AND 911 SERVICE

This dial plan example allows the DID number of any user on a system to be presented as an outbound Caller ID when that user dials 911. When the user makes any other type of outbound call, the Caller ID presented is the main number of the site.

To accomplish this:

1. Create a new extension list and, while doing so, assign as many PRI channels as there are devices to have a sufficient number for potential 911 calls.

   3Com strongly recommends that you use the highest-numbered channels for the 911 calls. The channels that you put in this list *must* be removed from the *0002 extension list to ensure that channels are available for emergency calls.

   *In the example in this appendix, Ext List *0011 and Route 11 are used.*

2. Once you have customized and imported your dial plan (see the example in the section), go to *Dial Plan > Pretranslators > Highlight "Outbound Caller ID for non-911 Calls" > Click Devices Using for CLI*.
3. Move to the left only the channels in *0002.

   These are the channels that will be used for non-911 calls.

4. Go to *Dial Plan > Pretranslators > Highlight "Outbound Caller ID for 911 Calls" > Click Devices Using for CLI*.
5. Move to the left *only* the channels that will be used for 911 calling.

   These will be the same channels as those designated in Ext List *0011.

Sample Dial Plan

Examine the sample dial plan in the rest of this appendix to learn the customized lines that deviate from the default dial plan.

Internal 3-Digit Extensions

This portion of the dial plan shows the 3-digit dial plan configuration.

```
Table Create  1 Internal 3 Digit Extensions
/                  Id Entry Digits       Min Max Class           Prio Route
/                  -- ----- ------------ --- --- -------------   ---- -----
TableEntry Create  1    1    0            1   1   Internal          0    4
TableEntry Create  1    2    1            3   3   Internal          0    0
TableEntry Create  1    3    2            3   3   Internal          0    0
TableEntry Create  1    4    3            3   3   Internal          0    0
TableEntry Create  1    5    4            3   3   Internal          0    0
TableEntry Create  1    6    5            3   3   Internal          0    3
TableEntry Create  1    7    6            3   3   Internal          0    0
TableEntry Create  1    8    7            3   3   Diagnostics       0    0
TableEntry Create  1    9    9            8   8   Local             0    1
TableEntry Create  1    10   90           2   64  Operator          0    1
TableEntry Create  1    11   901          4   64  International     0    1
TableEntry Create  1    12   91           9   12  LongDistance      0    1
TableEntry Create  1    13   9101         9   64  AlternateLong     0    1
TableEntry Create  1    14   911          3   3   Emergency         0    11
TableEntry Create  1    15   91800        12  12  TollFree          0    1
TableEntry Create  1    16   91888        12  12  TollFree          0    1
TableEntry Create  1    17   91877        12  12  TollFree          0    1
TableEntry Create  1    18   91900        12  12  Toll              0    1
TableEntry Create  1    19   91976        12  12  Toll              0    1
TableEntry Create  1    20   9911         4   4   Emergency         0    11
TableEntry Create  1    21   9411         4   4   Operator          0    1
TableEntry Create  1    22   9*           4   4   COCode            0    1
```

Incoming DID Section

This portion of the dial plan shows the Direct Inward Dialing and Auto Attendant configuration.

```
Table Create  2 Incoming DID and Auto Attendant
/                  Id Entry  Digits       Min Max Class           Prio Route
/                  -- -----  ------------ --- --- -------------   ---- -----
TableEntry Create  2    1    0            1   1   Internal          0    4
TableEntry Create  2    2    1            3   3   Internal          0    0
TableEntry Create  2    3    2            3   3   Internal          0    0
TableEntry Create  2    4    3            3   3   Internal          0    0
TableEntry Create  2    5    4            3   3   Internal          0    0
TableEntry Create  2    6    5            3   3   Internal          0    3
```

Least Cost Routing Portion This portion of the dial plan shows the Least Cost Routing configuration.

```
Table Create  3 Least Cost Routing
//////////////////////////////////////////////////////////////////////////
////// /        Routes
//////////////////////////////////////////////////////////////////////////

/                       Route Description
/                       ----- -----------
DestinationRoute Create     1  LocalCO
DestinationRoute Create     2  LocalCONoStrip
DestinationRoute Create     3  Voice Application
DestinationRoute Create     4  Attendant
DestinationRoute Create     5  H323 ConneXtions Ports
DestinationRoute Create     6  Virtual Tie Line (VTL) Ports
DestinationRoute Create     7  Reserved
DestinationRoute Create     8  8 Pool
DestinationRoute Create    11  Route for 911

/                            Route Entry DestinationExtension
/                            ----- ----- --------------------
DestinationRouteEntry Create     1     1   *0002
DestinationRouteEntry Create     1     2   *0001
DestinationRouteEntry Create     2     1   *0001
DestinationRouteEntry Create     3     1   *0003
DestinationRouteEntry Create     4     1   *0004
DestinationRouteEntry Create     5     1   *0005
DestinationRouteEntry Create     6     1   *0006
DestinationRouteEntry Create     7     1   *0003
DestinationRouteEntry Create     8     1   *0008
DestinationRouteEntry Create    11     1   *0011

/                                 Route Entry OperId Operation  Value
/                                 ----- ----- ------ ---------  -----
DestinationRouteOperation Create    1     1      1   stripLead  1
DestinationRouteOperation Create    1     2      1   stripLead  1
DestinationRouteOperation Create    8     1      1   stripLead  1
DestinationRouteOperation Create   11     1      1   replace    911
```

Pretranslators (Part 1) This portion of the dial plan shows the first part of the Pretranslators configuration.

```
////////////////////////////////////////////////////////////////////////
////// /        Pretranslators
////////////////////////////////////////////////////////////////////////

PreTranslator Create  1  4Digit DDI 3Digit Internal
/                         PreTransId Entry Digits
/                         ---------- ----- ------
PreTranslatorEntry Create     1       1    1
PreTranslatorEntry Create     1       2    2
PreTranslatorEntry Create     1       3    3
PreTranslatorEntry Create     1       4    4
PreTranslatorEntry Create     1       5    5
PreTranslatorEntry Create     1       6    6
PreTranslatorEntry Create     1       7    7
PreTranslatorEntry Create     1       8    8
PreTranslatorEntry Create     1       9    9
PreTranslatorEntry Create     1       10   0

PreTranslator Create  2  Outbound Caller ID for non-911 Calls
/                         PreTransId Entry Digits
/                         ---------- ----- ------
PreTranslatorEntry Create     2       1    1
PreTranslatorEntry Create     2       2    2
PreTranslatorEntry Create     2       3    3
PreTranslatorEntry Create     2       4    4

PreTranslator Create  3  Outbound Caller ID for 911 Calls
/                         PreTransId Entry Digits
/                         ---------- ----- ------
PreTranslatorEntry Create     3       1    1
PreTranslatorEntry Create     3       2    2
PreTranslatorEntry Create     3       3    3
PreTranslatorEntry Create     3       4    4
```

Pretranslators (Part2) This portion of the dial plan shows the second part of the Pretranslators configuration.

```
/                            PreTransId Entry OperId Operation  Value
/                            ---------- ----- ------ ---------  -----
PreTranslatorOperation Create    1        1       1   stripLead  1
PreTranslatorOperation Create    1        2       1   stripLead  1
PreTranslatorOperation Create    1        3       1   stripLead  1
PreTranslatorOperation Create    1        4       1   stripLead  1
PreTranslatorOperation Create    1        5       1   stripLead  1
PreTranslatorOperation Create    1        6       1   stripLead  1
PreTranslatorOperation Create    1        7       1   stripLead  1
PreTranslatorOperation Create    1        8       1   stripLead  1
PreTranslatorOperation Create    1        9       1   stripLead  1
PreTranslatorOperation Create    1        10      1   stripLead  1
PreTranslatorOperation Create    2        1       1   replace    5083232000
PreTranslatorOperation Create    2        2       1   replace    5083232000
PreTranslatorOperation Create    2        3       1   replace    5083232000
PreTranslatorOperation Create    2        4       1   replace    5083232000
PreTranslatorOperation Create    3        1       1   prepend    5083232
PreTranslatorOperation Create    3        2       1   prepend    5083232
PreTranslatorOperation Create    3        3       1   prepend    5083232
PreTranslatorOperation Create    3        4       1   prepend    5083232
```

G NBX ENTERPRISE MIB

This appendix shows the NBX Enterprise MIB, which defines the MIB objects that have a proprietary purpose on the system.

NCP refers to the Call Processor.

```
********************************************************************************
-- *
-- *     Copyright (c) 2003 by 3Com Corporation.
-- *     All Rights Reserved.
-- *
-- *
-- *     $Revision:  0.02 $
-- *     $Date:  11/08/2005     $
--
********************************************************************************

A3COMNBX-MIBDEFINITIONS ::= BEGIN
-- All definitions within this MIB are derived from the IANA assigned enterprise
-- which is declared under the enterprises node defined in the SNMP SMI.
   IMPORTS
      a3comNbxMIB
         FROM A3Com-products-MIB
   -- Import the ENTITY mib for showing the NBX hardware and software
versions,Serial Number.
      entPhysicalIndex,entPhysicalName
         FROM ENTITY-MIB
      PhysAddress, DisplayString
         FROM SNMPv2-TC
      DisplayString, ipAdEntAddr
         FROM RFC1213-MIB
      enterprises, MODULE-IDENTITY, OBJECT-TYPE, Integer32, IpAddress,
NOTIFICATION-TYPE, Counter32
         FROM SNMPv2-SMI;
```

```
   nbxMODULE-IDENTITY
      LAST-UPDATED"200603281714Z"-- mar 28 2006.
      ORGANIZATION"3Com"
      CONTACT-INFO"Postal: 350 Campus Drive
                Marlborough, MA 01752-3064
                phone: 508-323-5000
                fax: 508-323-1111"
      DESCRIPTION"The Module is meant to describe and store the information about
                the various objects that are defined for the Network business
exchange
                (NBX) box. This module includes the device information and the
statistics
                that are maintained by the NBX. These statistics include the
information on
                the Licenses added, IP and Qos Settings etc."
      REVISION"200511081714Z"
      DESCRIPTION""
      ::=  {  a3comNbxMIB  1  }

-- This MIB defines 3 groups that provide for the control and monitoring
-- of all parts of an NBX system and one group for notifications.

   nbxCallProcessorOBJECT IDENTIFIER
      ::=  {  nbx  1  }

   nbxGatewayOBJECT IDENTIFIER
      ::=  {  nbx  2  }

   nbxPhoneOBJECT IDENTIFIER
      ::=  {  nbx  3  }

   nbxNotificationsOBJECT IDENTIFIER
      ::=  {  nbx  4  }

-- The Call Processor Group
-- Implementation of this group is mandatory for all systems
-- The serial num, part number, SW version, HW version for the NCP
-- will be provided by the entity mib (rfc-2737) instead of creating a
-- private mib for it. Interface info on the NCP is provided by MIB-2.

   ncpSettingsOBJECT IDENTIFIER
      ::=  {  nbxCallProcessor  1  }

   ncpIPModeSettingsOBJECT-TYPE
      SYNTAX  INTEGER  {
                        layer2Only ( 1 ) ,
```

```
                        layer3Only ( 2 ) ,
                        iponFly ( 3 )
                      }
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The IP operating mode for connected NBX devices"
      ::=  {  ncpSettings  1  }

-- The  QOS settings group is required. These settings are not yet finalized, but
placed here
-- for the completeness of the document. Incase these are not available, these
-- will be removed
   ncpQosSettingsOBJECT IDENTIFIER
      ::=  {  ncpSettings  2  }

-- Provided the stats items as a table indexed by the 'entPhysicalIndex'
-- from the entity MIB. This way if we have a two board system we can show
-- these statistics for each.

   ncpTableOBJECT-TYPE
      SYNTAXSEQUENCE  OF  NcpEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"The Table consisit of one row for each NCP board available in the
NBX System."
      ::=  { nbxCallProcessor  2 }

   ncpEntryOBJECT-TYPE
      SYNTAXNcpEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"Indicates an Entry for each NCP in the NCP table."
      INDEX{  entPhysicalIndex  }
      ::=  { ncpTable 1 }

   NcpEntry  ::=  SEQUENCE {
      ncpNumberOfActiveCalls  Integer32,
      ncpIncomingVTLCallFailures  Counter32,
      ncpOutgoingVTLCallFailures  Counter32,
      ncpMemoryFree  DisplayString,
      ncpDosPartitionFree  DisplayString,
      ncpHtfsPartitionFree  DisplayString,
      ncpPowerStatus  INTEGER,
      ncpNumberOfVMPorts  Integer32
      }
```

```
   ncpNumberOfActiveCallsOBJECT-TYPE
      SYNTAXInteger32
      MAX-ACCESSread-only
      STATUScurrent
      DESCRIPTION"Indicates a number to track the number of active calls."
      ::=  {  ncpEntry  1  }


   ncpIncomingVTLCallFailuresOBJECT-TYPE
      SYNTAX  Counter32
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"Indicates a Counter to track the number of  Incoming VTL Call
Failures"
      ::=  {  ncpEntry  2  }


   ncpOutgoingVTLCallFailuresOBJECT-TYPE
      SYNTAX  Counter32
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"Indicates a Counter to track the number of Outgoing VTL Call
Failures"
      ::=  {  ncpEntry  3  }

-- Though the Memory free is in MB, to present the accurate value, it is better
-- to use the display string.
   ncpMemoryFreeOBJECT-TYPE
      SYNTAXDisplayString
      MAX-ACCESSread-only
      STATUScurrent
      DESCRIPTION"Indicates the free Memory in the system"
      ::=  {  ncpEntry  4  }

-- This is a display string as the number is greater than the maximum value
-- that an integer can store. The value is in GB. So better to display in
-- display string.
   ncpDosPartitionFreeOBJECT-TYPE
      SYNTAXDisplayString
      MAX-ACCESSread-only
      STATUScurrent
      DESCRIPTION"Indicates the Dos partition that is free"
      ::=  {  ncpEntry  5  }

-- This is a display string as the number is greater than the maximum value
-- that an integer can store. The value is in GB. So better to display in
```

```
-- display string.

   ncpHtfsPartitionFreeOBJECT-TYPE
      SYNTAXDisplayString
      MAX-ACCESSread-only
      STATUScurrent
      DESCRIPTION"Indicates the HTFS partition that is free"
      ::=  {  ncpEntry  6  }


-- The status of the power supply present in the NCP. In some of the NBX systems
there will
-- be two power supplies. This object indicates the status of each of the power
supply.

   ncpPowerStatusOBJECT-TYPE
      SYNTAX  INTEGER  {
                        ps1Failed ( 1 ) ,
                        ps2Failed ( 2) ,
                        allOk ( 3 )
                      }
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"Indicates the power status of the NCP when redundant
                  power supply is available."
      ::=  {  ncpEntry  7  }


   ncpNumberOfVMPorts OBJECT-TYPE
      SYNTAXInteger32
      MAX-ACCESSread-only
      STATUScurrent
      DESCRIPTION"Indicates the number of voicemail ports that are present in the
                 NBX"
      ::=  {  ncpEntry  8  }


-- The Operations table starts from here. This is used for doing a NCP reboot  or
shutdown.
   ncpOperationTableOBJECT-TYPE
      SYNTAXSEQUENCE OF NcpOperationEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"This table consists of objects meant for rebooting and
                   shutting down the NBX system."
      ::=  {  nbxCallProcessor  3  }
```

```
   ncpOperationEntryOBJECT-TYPE
      SYNTAXNcpOperationEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"Indicates an Entry for the operations table."
      INDEX{ entPhysicalIndex }
      ::={ ncpOperationTable 1}

   NcpOperationEntry  ::=  SEQUENCE {
      ncpOperationReboot  INTEGER,
      ncpOperationShutDown  INTEGER
      }
   -- For this version, we are not supporting the scheduled reboot and shut
        -- down features
   ncpOperationRebootOBJECT-TYPE
      SYNTAX  INTEGER {
                                              inActive(1),
                          active(2)
                      }
      MAX-ACCESSread-write
      STATUScurrent
      DESCRIPTION"This object is used to set the NCP to reboot. When set to
              active(2) the NBX is rebooted. When a GET is done, then
              the inActive(1) is returned indicating the current
              status."
      ::=  {  ncpOperationEntry  1  }

    ncpOperationShutDownOBJECT-TYPE
      SYNTAX  INTEGER {
                                                    inActive(1),
                                                    active(2)
                                               }
      MAX-ACCESSread-write
      STATUS  current
      DESCRIPTION"This object is used to set the NCP to Shut Down. When set
                          to active(2) the NCP is Shut down. When a GET
                          is done then the inActive(1) is returned."
      ::=  {  ncpOperationEntry  2  }

-- The licenses table starts from here.
   ncpLicenseTableOBJECT-TYPE
      SYNTAXSEQUENCE  OF  NcpLicenseEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
```

```
      DESCRIPTION" The table consists of the licenses that are in use and the purpose
used
            for in the  NBX system"
      ::=  { nbxCallProcessor  4 }

   ncpLicenseEntryOBJECT-TYPE
      SYNTAXNcpLicenseEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"Indicates an Entry for the Licenses table."
      INDEX{  ncpLicenseIndex  }
      ::=  { ncpLicenseTable 1 }

   NcpLicenseEntry  ::=  SEQUENCE {
      ncpLicenseIndex  Integer32,
      ncpLicenseName  INTEGER,
      ncpLicenseDescription  DisplayString,
      ncpLicenseTotal  Integer32,
      ncpLicenseInUse  Integer32
      }

   ncpLicenseIndexOBJECT-TYPE
      SYNTAX  Integer32
      MAX-ACCESSnot-accessible
      STATUS  current
      DESCRIPTION"The License Index is a unique number to distinguish
              the licenses that are present in the NBX system"
      ::=  {  ncpLicenseEntry  1  }

-- The License name is indicative of the feature for which respective access is
enabled.
-- these are taken from License.cpp file.
-- Because of some limitations the voicemail feature codes are abbrievated. for
example, the code
-- vmNbx100Upg4H4PFrom30M4P should be read as voice mail upgraded to 4 Hrs 4 Ports
From 30min 4Ports.
-- vmNbx100Upg20H6PFrom30M4P should be read as voice mail upgraded to 20 Hours 6
Ports from 30 min 4 ports .
-- vm denotes voicemail,P for ports,H for Hours, M for Min.
   ncpLicenseNameOBJECT-TYPE
      SYNTAX  INTEGER {
                           deviceCount(1),
                                                   diskMirroring(2),
                                                   voiceMail(3),
                                                   vmPortCount(4),
                                                   vmNbx100Upg4H4PFrom30M4P(5),
```

```
                                        vmNbx100Upg20H6PFrom30M4P(6),
                                        vmNbx100UpgMaxH12PFrom30M4P(7),
                                        vmNbx100Upg20H6PFrom4H4P(8),
                                        vmNbx100UpgMaxH12PFrom4H4P(9),
                                        vmNbx100UpgMaxH12PFrom20H6P(10),
                                        ip(11),
                                        ipStandard(12),
                                        ipOnTheFly(13),
                                        ipUpgrade(14),
                                        h323NTCount(15),
                                        softphoneCount(16),
                                        wavDeviceCount(17),
                                        vtlPortCount(18),
                                        vpim(19),
                                        thirdPartyMsg(20),
                                        cas(21),
                                        callRecordMonitor(22),
                                        tpPolycomCount(23),
                                        tpCitelNorstar(24),
                    vmNbx100DefaultLicense(26),
                                        starFish(28),
                    softwareUpgrade(29),
                    citelAvaya2GatewayLicense(30),
                    tpCitelAnalog(31),
                                        citelOther2Gateway(32),
                                        citelOther3Gateway(33),
                                        desoto(34),
                    basicPhone3101(36),
                                        group2(37),
                                        group1(38),
                                        group0(40),
                                        group3(43),
                                        group4(44),
                                        nbxACD(45),
                bri2portto4port(46),
                v3001RDiskMirroringKit(47),
                invalidLicense(48),
                unknownLicense(49)
                                    }

    MAX-ACCESSread-only
    STATUS  current
    DESCRIPTION"The license Name for which the access is allowed. It is an
enumerated type
            which represents the corresponding License."
    ::=  {  ncpLicenseEntry  2  }
```

```
   ncpLicenseDescriptionOBJECT-TYPE
      SYNTAX  DisplayString
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The description of the License."
      ::=  {  ncpLicenseEntry  3  }


   ncpLicenseTotalOBJECT-TYPE
      SYNTAX  Integer32
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The Total Number of devices available to be used in the system
using the particular
                license."
      ::=  {  ncpLicenseEntry  4  }


   ncpLicenseInUseOBJECT-TYPE
      SYNTAX  Integer32
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The total number of units that are being used in system."
      ::=  {  ncpLicenseEntry  5  }


-- The Gateways Group, This group is one of the groups configured under nbx object
identifier.
-- Implementation of this group is mandatory for all systems
-- This group contains a Table of all the gateways that form part of an nbx system.

-- The NCP discovers and proxies the configuration specific to digital
-- or analog gateways.

   gatewayTableOBJECT-TYPE
      SYNTAXSEQUENCE  OF  GatewayEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"The table consists of the list of gateway devices that are
connected to the NBX. This list
                  includes the List of TLIM,PRI, BRI, ATC etc. The device class will
differentiate the type of device
                   attached to the NBX."
      ::=  { nbxGateway  1 }
```

```
   gatewayEntryOBJECT-TYPE
      SYNTAXGatewayEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"Indicates an Entry for each gateway in the Gateway table."
      INDEX{  gatewayDeviceId  }
      ::=  { gatewayTable 1 }

   GatewayEntry  ::=  SEQUENCE {
      gatewayDeviceId    Integer32,
      gatewayMacAddress  PhysAddress,
      gatewayClass  INTEGER,
      gatewaySerialNumber  DisplayString,
      gatewayPartNumber  DisplayString,
      gatewayHWVersion  DisplayString,
      gatewaySWVersion  DisplayString,
      gatewayIPAddress  IpAddress,
      gatewayIPMask  IpAddress,
      gatewayIPGateway  IpAddress,
      gatewayDescription  DisplayString,
      gatewayDeviceName  DisplayString,
      gatewayStatus  INTEGER,
      gatewayNumberOfChannels  Integer32,
      gatewayModelNumber  DisplayString,
      gatewayReboot  INTEGER
      }

-- The gateway class is meant to indicate the type of gateway present in the system.
-- The enum other indicates any other gateway that is present in the system other
than
-- the T1,ISDN PRI,BRI cards that are generally supported.
   gatewayDeviceIdOBJECT-TYPE
      SYNTAX  Integer32 ( -2147483648 .. 2147483647  )
      MAX-ACCESSnot-accessible
      STATUS  current
      DESCRIPTION"The Device ID of the Gateway connected to the NBX."
      ::=  {  gatewayEntry  1  }


   gatewayMacAddressOBJECT-TYPE
      SYNTAX  PhysAddress
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The MAC address of the Gateway connected to the NBX."
      ::=  {  gatewayEntry  2  }
```

```
-- The enums that are given here are as mentioned in the dbconst.h. Changing the
order will
-- effect the complexity of code for handling the enums.

   gatewayClassOBJECT-TYPE
      SYNTAX  INTEGER {
                        tlimGrowler(4),
                        tlimProto(5),
                         tlimAlpha(6),
                        tlimH323(13),
                        ata(15),
                        t1(16),
                        t1Channel(17),
                        isdnBRI(18),
                       chasis(31),
                       trunkGroup(36),
                       trunkSpan(37),
                       trunkPriSpan(40),
                       trunkBriSpan(41),
                       trunkPriChannel(42),
                       trunkBriChannel(43),
                       trunkPriGroup(44),
                       trunkBriGroup(45),
                       trunkDSP(46),
                       ataMorticia(58),
                       tlimGomez(59),
                       trunkPriDChannel(61),
                       trunkBriDChannel(62),
                       ataThirdPart(63),
                       ataWednesday(64),
                       trunkSpanLoopback(65),
                       trunkPriSpanLoopback(66),
                       ataSkylark(94),
                       unknownGatewayClass(100),
                       isdnPRI(101)
                      }
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"An enumeration for E1,T1,PRI,BRI,ATA etc."
      ::=  {  gatewayEntry  3  }


   gatewaySerialNumberOBJECT-TYPE
      SYNTAX  DisplayString
      MAX-ACCESSread-only
      STATUS  current
```

```
   DESCRIPTION"The 3Com 13 digit Serial Number present on the gateway."
   ::=  {  gatewayEntry  4  }


gatewayPartNumberOBJECT-TYPE
   SYNTAX  DisplayString
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The 3C Part Number of the Gateway."
   ::=  {  gatewayEntry  5 }


gatewayHWVersionOBJECT-TYPE
   SYNTAX  DisplayString
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The hardware verison of the gateway."
   ::=  {  gatewayEntry  6  }


gatewaySWVersionOBJECT-TYPE
   SYNTAX  DisplayString
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The Software Version of the gateway."
   ::=  {  gatewayEntry  7  }


gatewayIPAddressOBJECT-TYPE
   SYNTAX  IpAddress
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The IP Address of the Gateway."
   ::=  {  gatewayEntry  8  }


gatewayIPMaskOBJECT-TYPE
   SYNTAX  IpAddress
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The IP mask of the respective Gateway connected to the NBX."
   ::=  {  gatewayEntry  9  }


gatewayIPGatewayOBJECT-TYPE
   SYNTAX  IpAddress
```

```
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The IP Gateway address of the gateway."
      ::=  {  gatewayEntry  10  }


   gatewayDescriptionOBJECT-TYPE
      SYNTAX  DisplayString
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The Description about the Gateway that is connected to the NBX."
      ::=  {  gatewayEntry  11  }


   gatewayDeviceNameOBJECT-TYPE
      SYNTAX  DisplayString
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The name of the gateway ."
      ::=  {  gatewayEntry  12  }

-- The enums that are given here are as mentioned in the dbconst.h. Changing the
order will
-- effect the complexity of code for handling the enums.
   gatewayStatusOBJECT-TYPE
      SYNTAX  INTEGER {
                                              online(1),
                                              offline(3),
                                              unknownGatewayStatus(100)
                                             }
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"An enumeration that gives the status of the gateway, as
online,offline,unknown,etc."
      ::=  {  gatewayEntry  13  }


   gatewayNumberOfChannelsOBJECT-TYPE
      SYNTAX  Integer32
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The Number of channels or ports that are onboard for the
corresponding Gateway."
      ::=  {  gatewayEntry  14  }
```

```
   gatewayModelNumberOBJECT-TYPE
      SYNTAX  DisplayString
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The  model number of the gateway."
      ::=  {  gatewayEntry  15 }

-- The gateway reboot will allow the users to set the respective gateway to  reboot.

   gatewayRebootOBJECT-TYPE
      SYNTAX  INTEGER {
                       inActive(1),
                       active(2)
                      }
      MAX-ACCESSread-write
      STATUS  current
      DESCRIPTION"The object will allow users to reboot the specific gateway. Setting
the object
                                  with active(2) will reboot the respective gateway."
      ::=  {  gatewayEntry  16  }

-- nbxDlC is in the gateway group. It gives the span and channel information of
digital line cards that
-- are connected to the nbx.
   gatewayDLCOBJECT IDENTIFIER
      ::=  {  nbxGateway  2  }

   dlcSpanTableOBJECT-TYPE
      SYNTAXSEQUENCE  OF  DlcSpanEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"This table gives the information of the span entries of various
Digital line cards  that are connected to the nbx."
      ::=  { gatewayDLC  1 }

   dlcSpanEntryOBJECT-TYPE
      SYNTAXDlcSpanEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"Indicates an entry for each of the Span in the DLC"
      INDEX{  dlcSpanDeviceId }
      ::=  { dlcSpanTable 1 }

   DlcSpanEntry  ::=  SEQUENCE {
      dlcSpanDeviceId Integer32,
      dlcSpanMACAddress  PhysAddress,
```

```
   dlcSpanID  Integer32,
   dlcSpanName  DisplayString,
   dlcSpanSignalProtocol  INTEGER,
   dlcSpanFraming  INTEGER,
   dlcSpanLineCode INTEGER,
   dlcSpanLineLength  INTEGER,
   dlcSpanTimingMode  INTEGER,
   dlcSpanNumberOfChannels  Integer32,
   dlcSpanNumberOfChannelsOnline  Integer32,
   dlcSpanNumberOfChannelsOffline  Integer32,
   dlcSpanStatus  INTEGER,
   dlcSpanTEIManualAuto INTEGER,
   dlcSpanTEIId DisplayString
   }

dlcSpanDeviceIdOBJECT-TYPE
   SYNTAX  Integer32  ( -2147483648 .. 2147483647  )
   MAX-ACCESSnot-accessible
   STATUS  current
   DESCRIPTION"The span device ID is a unique number
                   that identifies the respective span."
   ::=  {  dlcSpanEntry  1  }
dlcSpanMACAddressOBJECT-TYPE
   SYNTAX  PhysAddress
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The MAC address of the Span."
   ::=  {  dlcSpanEntry  2  }

dlcSpanIDOBJECT-TYPE
   SYNTAX  Integer32  ( -2147483648 .. 2147483647  )
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The span device ID is a unique Virtual device number
                   that identifies the respective span."
   ::=  {  dlcSpanEntry  3  }

dlcSpanNameOBJECT-TYPE
   SYNTAX  DisplayString
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The name of the span configured in the
           NBX."
   ::=  {  dlcSpanEntry  4  }
```

```
-- The enums that are given here are as mentioned in the gNipTep.h. Changing the
order will
-- effect the complexity of code for handling the enums.
   dlcSpanSignalProtocolOBJECT-TYPE
      SYNTAX  INTEGER {
                      ess5(1),
                      dms(2),
                      ni2(3),
                      qSigSlave(4),
                      qSigMaster(5),
                      t1QSigSlave(6),
                      t1QsigMaster(7),
                      ess4(8),
                      etsi(9) ,
                      protocolNotApplicable(100)
                      }
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"Describes the Protocol used
                by the span."
      ::=  {  dlcSpanEntry  5  }
-- The enums that are given here are as mentioned in the gNipTep.h. Changing the
order will
-- effect the complexity of code for handling the enums.

   dlcSpanFramingOBJECT-TYPE
      SYNTAX  INTEGER {
                        crcmf(1),
                        f4mf(2),
                        f12mf(3),
                        esf(4),
                        f72mf(5),
                        d4(6),
                        df(7),
                        framingNotApplicable(100)
                      }
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"Enumeration describing the Framing type
                used by the card."
      ::=  {  dlcSpanEntry  6  }

-- The enums that are given here are as mentioned in the gNipTep.h. Changing the
order will
-- effect the complexity of code for handling the enums.
   dlcSpanLineCodeOBJECT-TYPE
```

```
   SYNTAX  INTEGER {

                     hdb3(1),
                     b8zs(2),
                     ami(3) ,
                     lineCodeNotApplicable(100)
                    }
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The line code used by the span."
   ::=  {  dlcSpanEntry  7  }


dlcSpanLineLengthOBJECT-TYPE
   SYNTAX  INTEGER
                   {
                   t1_len_000035(1),
                   t1_len_025056(2),
                   t1_len_055095(3),
                   t1_len_085125(4),
                   t1_len_115155 (5),
                   t1_len_145185 (6),
                   t1_len_175210(7),
                   t1_len_dbLongHaul(8),
                   t1_len_7dbLongHaul(9),
                   t1_len_15dbLongHaul(10),
                   t1_len_22dbLongHaul(11),
                   pri_len_000035(51),
                   pri_len_025056(52),
                   pri_len_055095(53),
                   pri_len_085125(54),
                   pri_len_115155 (55),
                   pri_len_145185 (56),
                   pri_len_175210(57),
                   pri_len_NA(58),
                   pri_len_dbLongHaul(59),
                   pri_len_7dbLongHaul(60),
                   pri_len_15dbLongHaul(61),
                   pri_len_22dbLongHaul(62),
                   lineLengthNotApplicable(100)
                   }
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The span line length used by the card."
   ::=  {  dlcSpanEntry  8  }
```

```
dlcSpanTimingModeOBJECT-TYPE
   SYNTAX  INTEGER {

                     internal(1) ,
                     loop(2),
                     timingModeNotApplicable(100)
                   }
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The timing mode configured for the
                    Span."
   ::=  {  dlcSpanEntry  9  }


dlcSpanNumberOfChannelsOBJECT-TYPE
   SYNTAX  Integer32
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The number of channels that are present
                  in the card,"
   ::=  {  dlcSpanEntry  10  }


dlcSpanNumberOfChannelsOnlineOBJECT-TYPE
   SYNTAX  Integer32
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The number of channels that are online
             in the span list of the card,"
   ::=  {  dlcSpanEntry  11  }


dlcSpanNumberOfChannelsOfflineOBJECT-TYPE
   SYNTAX  Integer32
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The number of channels that are offline
                  in the card."
   ::=  {  dlcSpanEntry  12  }


dlcSpanStatusOBJECT-TYPE
   SYNTAX  INTEGER {
                                            online(1),
                                            offline(3),
```

```
                                                unknownSpanStatus(100)
                                               }
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The status of the span, whether
                  online, offline, unknown, etc."
      ::=  {  dlcSpanEntry  13 }
-- This object exists only for BRI Span. For the other spans i could not find a
-- mention of that.

   dlcSpanTEIManualAuto OBJECT-TYPE
      SYNTAX  INTEGER {
                        manual(1),
                        auto(2) ,
                        notApplicable(100)
                       }
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The status of the TEI Assignment. If it is
                configured to automatic then auto(2) is returned else
               manual(1) is returned. If it doesnot exist notApplicable is returned."
      ::={ dlcSpanEntry    14}


   dlcSpanTEIIdOBJECT-TYPE
      SYNTAX  DisplayString
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION" The TEI ID of the span if exists."
      ::={ dlcSpanEntry     15}

   dlcChannelTableOBJECT-TYPE
      SYNTAXSEQUENCE  OF  DlcChannelEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"This table consists of the details regarding the channels
              in the NBX. These include the T1,E1,PRI,BRI etc."
      ::=  { gatewayDLC  2 }

   dlcChannelEntryOBJECT-TYPE
      SYNTAXDlcChannelEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"Indicates an entry for each of the Channel in the DLC"
      INDEX{  dlcChannelDeviceId  }
      ::=  { dlcChannelTable 1 }
```

```
DlcChannelEntry  ::=  SEQUENCE {
   dlcChannelDeviceId Integer32,
   dlcChannelMAC  PhysAddress,
   dlcChannelID  Integer32,
   dlcChannelGroupName  DisplayString,
   dlcChannelName  DisplayString,
   dlcChannelSpanId  Integer32,
   dlcChannelExtension  Integer32,
   dlcChannelProtocolINTEGER,
   dlcChannelDirection  INTEGER,
   dlcChannelstartType  INTEGER,
   dlcChannelIncomingDigitFormat  INTEGER,
   dlcChannelCalledPartyDigits  Integer32,
   dlcChannelOutgoingDigitFormat  INTEGER,
   dlcChannelAutoExt  Integer32,
   dlcChannelStatus  INTEGER,
   dlcChannelRestart INTEGER,
   dlcChannelErrorCountCounter32,
   dlcChannelLastErrorCode DisplayString
   }

dlcChannelDeviceIdOBJECT-TYPE
   SYNTAX  Integer32
   MAX-ACCESSnot-accessible
   STATUS  current
   DESCRIPTION"The Channel device Id gives the unique number
               that identifies the channel
               appropriately."
   ::=  {  dlcChannelEntry  1  }

dlcChannelMACOBJECT-TYPE
   SYNTAX  PhysAddress
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The MAC address of the channel."
   ::=  {  dlcChannelEntry  2  }

dlcChannelIDOBJECT-TYPE
   SYNTAX  Integer32
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The Channel ID gives the unique virtual device number
           that identifies the channel
               appropriately."
   ::=  {  dlcChannelEntry  3  }
```

```
dlcChannelGroupNameOBJECT-TYPE
   SYNTAX  DisplayString
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The group name of the channel"
   ::=  {  dlcChannelEntry 4  }


dlcChannelNameOBJECT-TYPE
   SYNTAX  DisplayString
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The Name of the DLC channel ."
   ::=  {  dlcChannelEntry  5  }


dlcChannelSpanIdOBJECT-TYPE
   SYNTAX  Integer32
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The Span Id of the  channel."
   ::=  {  dlcChannelEntry  6  }


dlcChannelExtensionOBJECT-TYPE
   SYNTAX  Integer32
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The Extension of the channel."
   ::=  {  dlcChannelEntry  7  }

dlcChannelProtocolOBJECT-TYPE
   SYNTAX  INTEGER {
                     did(1),
                     fxo(2),
                     fxs(3),
                     gnd(4),
                     sigModeClearChannel(5),
                     em(6),
                     channelProtocolNotApplicable(100)
                    }
   MAX-ACCESS       read-only
   STATUS  current
   DESCRIPTION"The Protocol used by the channel."
   ::= {   dlcChannelEntry 8}
```

```
dlcChannelDirectionOBJECT-TYPE
   SYNTAX  INTEGER {
                    inOnly(1),
                    twoWay(2),
                    channelDirectionNotApplicable(100)
                   }
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The direction of the channel, Indicates
           if it is one way or two way."
   ::=  {  dlcChannelEntry  9  }


dlcChannelstartTypeOBJECT-TYPE
   SYNTAX  INTEGER {
                                                immediate(1),
                                                delay(2),
                                                dialTone(3),
                                                wink(4),
                     channelStartTypeNotApplicable(100)
                                               }
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"Indicates the start type of the
           channel."
   ::=  {  dlcChannelEntry  10  }


dlcChannelIncomingDigitFormatOBJECT-TYPE
   SYNTAX  INTEGER {
                    pulse(1),
                    dnis(2),
                    dnisAni(3),
                    sDnis(4),
                    sDnisAnis(5),
                    sAnisDnis(6),
                    dtmf(7),
                    incomingDigitFormatNotApplicable(100)
                    }
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"Indicates the incoming digit format of
           the channel, whether DNIS, ANI etc."
   ::=  {  dlcChannelEntry  11  }
```

```
   dlcChannelCalledPartyDigitsOBJECT-TYPE
      SYNTAX  Integer32
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"Gives the called party digits."
      ::=  {  dlcChannelEntry  12  }


   dlcChannelOutgoingDigitFormatOBJECT-TYPE
      SYNTAX  INTEGER {
                        pulse(1),
                        dnis(2),
                        dnisAni(3),
                        sDnis(4),
                        sDnisAnis(5),
                        sAnisDnis(6),
                        dtmf(7),
                        outgoingDigitFormatNotApplicable(100)
                       }
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"Gives the outgoing digit format configured for the channel."
      ::=  {  dlcChannelEntry  13  }


   dlcChannelAutoExtOBJECT-TYPE
      SYNTAX  Integer32
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The auto extension configured for the channel."
      ::=  {  dlcChannelEntry  14  }


   dlcChannelStatusOBJECT-TYPE
      SYNTAX  INTEGER {
                                                 online(1),
                                               offline(3),
                                               unknownChannelStatus(100)
                                              }
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The status of the respective Channel. Gives whether it is online or
offline
                  etc."
      ::=  {  dlcChannelEntry  15  }
```

```
   dlcChannelRestart   OBJECT-TYPE
      SYNTAX  INTEGER {
                        inActive(1),
                        active(2)
                      }
      MAX-ACCESSread-write
      STATUS  current
      DESCRIPTION        "when set to active(2), the channel is restarted"
      ::=  {  dlcChannelEntry  16 }

   dlcChannelErrorCountOBJECT-TYPE
      SYNTAX  Counter32
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The counter to track the number of times errors
                 occured in the channel"
      ::={  dlcChannelEntry 17 }

   dlcChannelLastErrorCode  OBJECT-TYPE
      SYNTAX  DisplayString
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The Last error code returned by the channel"
      ::=  {  dlcChannelEntry  18 }

-- The analog line entries are described here. These entries give the analog
-- line details for ALC,ATA etc.

   gatewayAnalogLineOBJECT IDENTIFIER
      ::=  {  nbxGateway  3  }

   analogLineTableOBJECT-TYPE
      SYNTAXSEQUENCE  OF  AnalogLineEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"This table consists of the details
           regarding the Analog line card present in the NBX."
      ::=  { gatewayAnalogLine  1 }
-- Here 2 indexes are there one the lineId which indicates the Port number or line
number
-- and the other denotes the mac address of the analog line card.
   analogLineEntryOBJECT-TYPE
      SYNTAXAnalogLineEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
```

```
      DESCRIPTION"Indicates an entry for each line or port present in the
              Line card"
      INDEX{ analogDeviceId  }
      ::=  { analogLineTable 1 }

   AnalogLineEntry  ::=  SEQUENCE {
      analogDeviceIdInteger32,
      analogLineMACAddress  PhysAddress,
      analogLineID  Integer32,
      analogLineExtension  Integer32,
      analogLineStatus  INTEGER,
      analogLineDeviceName  DisplayString
      }

   analogDeviceIdOBJECT-TYPE
      SYNTAX  Integer32
      MAX-ACCESSnot-accessible
      STATUS  current
      DESCRIPTION"The Analog Device ID gives the unique number that identifies
                the line appropriately."
      ::=  {  analogLineEntry  1  }

   analogLineMACAddressOBJECT-TYPE
      SYNTAX  PhysAddress
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The Mac address of the ALC card to which the line
                                  belongs to"
      ::=  {  analogLineEntry  2 }

   analogLineIDOBJECT-TYPE
      SYNTAX  Integer32
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The Analog line ID gives the unique Port number that identifies
                the line appropriately."
      ::=  {  analogLineEntry  3  }

   analogLineExtensionOBJECT-TYPE
      SYNTAX  Integer32
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The Analog Line card Extension gives the extension being used by
the
                line or port."
      ::=  {  analogLineEntry  4  }
```

```
-- enums taken from gNipTep.h
   analogLineStatusOBJECT-TYPE
      SYNTAX  INTEGER {
                        online(1),
                                                offline(3),
                                                unknownLineStatus(100)
                                                   }
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The port or line status,i.e information whether the
                  line is online or offline etc."
      ::=  {  analogLineEntry  5  }


   analogLineDeviceNameOBJECT-TYPE
      SYNTAX  DisplayString
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The Name of the port or line configured in theNBX."
      ::=  {  analogLineEntry  6 }

--The SIP Endpoints table starts from here

   gatewaySIPEndPointTableOBJECT-TYPE
      SYNTAXSEQUENCE  OF  GatewaySIPEndPointEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"This table consists of the details
           regarding the SIP Endpoints connected to the NBX."
      ::=  {  nbxGateway  4  }
-- The device Id of the sip endpoint is the index of the table
   gatewaySIPEndPointEntryOBJECT-TYPE
      SYNTAXGatewaySIPEndPointEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"Indicates an entry for each SIP endpoint present Connected to
              NBX"
      INDEX{ gatewaySIPEndPointDeviceId  }
      ::=  { gatewaySIPEndPointTable 1 }

   GatewaySIPEndPointEntry  ::=  SEQUENCE {
      gatewaySIPEndPointDeviceIdInteger32,
      gatewaySIPEndPointIPAddressIpAddress,
      gatewaySIPEndPointPortNumberInteger32,
      gatewaySIPEndPointDeviceName  DisplayString,
```

```
      gatewaySIPEndPointDescription  DisplayString
      }

   gatewaySIPEndPointDeviceId  OBJECT-TYPE
      SYNTAX  Integer32
      MAX-ACCESSnot-accessible
      STATUS  current
      DESCRIPTION"The Device ID of the SIP endpoint."
      ::=  {  gatewaySIPEndPointEntry  1  }

   gatewaySIPEndPointIPAddress  OBJECT-TYPE
      SYNTAX  IpAddress
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The IP address of the SIP endpoint."
      ::=  {  gatewaySIPEndPointEntry  2  }

   gatewaySIPEndPointPortNumber  OBJECT-TYPE
      SYNTAX  Integer32
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The port number being used by the SIP endpoint."
      ::=  {  gatewaySIPEndPointEntry  3  }

   gatewaySIPEndPointDeviceNameOBJECT-TYPE
      SYNTAX  DisplayString
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The name of the SIP endpoint."
      ::=  {  gatewaySIPEndPointEntry  4  }

   gatewaySIPEndPointDescriptionOBJECT-TYPE
      SYNTAX  DisplayString
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The description of the SIP endpoint."
      ::=  {  gatewaySIPEndPointEntry  5  }


-- The phone Table group starts from here.

   phoneTableOBJECT-TYPE
      SYNTAXSEQUENCE  OF  PhoneEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"The table consists of the list of phones
```

```
            that are connected to the NBX. This list
            includes the List of phones  etc. The device class will differentiate
            the type of device attached to the NBX."
      ::=  { nbxPhone  1 }

-- The mac address may become a problem for SIP phones, but we have no other
-- alternative other than device id, which, is not that meaningful.
   phoneEntryOBJECT-TYPE
      SYNTAXPhoneEntry
      MAX-ACCESSnot-accessible
      STATUScurrent
      DESCRIPTION"Indicates an entry for each phone present in the NBX"
      INDEX{ phoneDeviceId  }
      ::=  {phoneTable 1 }

   PhoneEntry  ::=  SEQUENCE {
      phoneDeviceIdInteger32,
      phoneMACAddress  PhysAddress,
      phoneVDN Integer32,
      phoneClass  INTEGER,
      phoneExtension  DisplayString,
      phoneSerialNumber  DisplayString,
      phonePartNumber  DisplayString,
      phoneHWVersion  DisplayString,
      phoneSWVersion  DisplayString,
      phoneIPAddress  IpAddress,
      phoneIPMask  IpAddress,
      phoneIPGateway  IpAddress,
      phoneDescription  DisplayString,
      phoneDeviceName  DisplayString,
      phoneStatus  INTEGER
      }

   phoneDeviceIdOBJECT-TYPE
      SYNTAX  Integer32
      MAX-ACCESSnot-accessible
      STATUS  current
      DESCRIPTION"The Device ID of the Phone or ATA device."
      ::=  {  phoneEntry  1  }

   phoneMACAddressOBJECT-TYPE
      SYNTAX  PhysAddress
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The MAC Address of the Phone device."
      ::=  {  phoneEntry  2  }
```

```
   phoneVDNOBJECT-TYPE
      SYNTAX  Integer32
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"The vdn of the ATA device.For phones it will be zero.For SIP
Devices
                  it indicates the port number being used."
      ::=  {  phoneEntry  3  }

-- The phone class is an enumeration which denotes the phone class to which it
belongs to.
-- These enums are given as mentioned in the dbconst.h. Changing the order will
-- effect the complexity of code for handling the enums. So we prefer it being this
way.
   phoneClassOBJECT-TYPE
      SYNTAX  INTEGER {
                                    nbSetGrowler(1),
                        nbSetProto(2),
                        nbSetAlpha(3),
                        nbSetBusiness(4),
                                                        nbSetSoft(15),
                        ata(16),
                        nbSetWav(48),
                                              basicSet(49),
                                              thirdParty1(51),
                                              thirdParty2(52),
                                              thirdParty3(53),
                                              thirdParty4(54),
                                              thirdParty5(55),
                                              thirdParty6(56),
                                              thirdParty7(57),
                                              thirdParty8(58),
                        ataMorticia(59),
                                              ataThirdParty1(64),
                        ataWednesday(65),
                        nbSet3102Business(66),
                                              cordlessPhone(67),
                                              basicSet3101(70),
                                              singleLineSet3100(75),
                                              managerPhone3103(77),
                        softPhone3102(80),
                        wirelessPhone3108(81),
                        convergenceClient(83),
                        thirdPartySIPPhone(85),
                        basicSet3101B(92),
```

```
                    basicSet3102B(93),
                    ataSkylark(95),
                    managerPhone3103B(96),
                    singleLineSet3100B(97),
                    unknownPhoneClass(100)
                                                }
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"An enumeration for describing the class of phone as basic,
              bussines, desoto phone etc"
   ::=  {  phoneEntry  4  }

phoneExtensionOBJECT-TYPE
   SYNTAX  DisplayString
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The Extension number of the phone."
   ::=  {  phoneEntry  5  }

phoneSerialNumberOBJECT-TYPE
   SYNTAX  DisplayString
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The 3COM 13 digit S/N"
   ::=  {  phoneEntry  6  }


phonePartNumberOBJECT-TYPE
   SYNTAX  DisplayString
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The 3C Part Number of the device."
   ::=  {  phoneEntry  7  }


phoneHWVersionOBJECT-TYPE
   SYNTAX  DisplayString
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The Hardware version of the Phone."
   ::=  {  phoneEntry  8  }


phoneSWVersionOBJECT-TYPE
   SYNTAX  DisplayString
   MAX-ACCESSread-only
```

```
   STATUS  current
   DESCRIPTION"The software version of the Phone."
   ::=  {  phoneEntry  9  }


phoneIPAddressOBJECT-TYPE
   SYNTAX  IpAddress
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The IP address of the Phone."
   ::=  {  phoneEntry  10  }


phoneIPMaskOBJECT-TYPE
   SYNTAX  IpAddress
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The IP mask of the Phone  Device."
   ::=  {  phoneEntry  11  }


phoneIPGatewayOBJECT-TYPE
   SYNTAX  IpAddress
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The IP gateway address of the phone device,"
   ::=  {  phoneEntry  12  }


phoneDescriptionOBJECT-TYPE
   SYNTAX  DisplayString
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"Description for the phone "
   ::=  {  phoneEntry  13 }


phoneDeviceNameOBJECT-TYPE
   SYNTAX  DisplayString
   MAX-ACCESSread-only
   STATUS  current
   DESCRIPTION"The name configured for the Phone device."
   ::=  {  phoneEntry  14  }


phoneStatusOBJECT-TYPE
```

```
      SYNTAX  INTEGER {
                                                  online(1),
                                              offline(3),
                                              unknownPhoneStatus(100)
                                                  }
      MAX-ACCESSread-only
      STATUS  current
      DESCRIPTION"An enumeration for giving information on status of the phone."
      ::=  {  phoneEntry  15  }


-- The Notifications Group Begins here.
-- The power status object is associated to the ncpPowerStatus object from the NCP
table
-- along with the physical name of the entity. Most of the NCP related notifications
are associated to
-- the entPhysicalName so as to inform the manager of the NCP that is sending the
notification
-- incase there are 2 NCP's available. By default the index of the table will be
-- mentioned in the notification if it is associated with the table object.
   notifyPowerStatusChangeNOTIFICATION-TYPE
      OBJECTS { entPhysicalName,ncpPowerStatus }
      STATUS  current
      DESCRIPTION"Notifies if the one of the redundant power supplies status changes
                from on to off and vice versa."
      ::=  {  nbxNotifications  1  }
-- The IP address is accessed from the MIB 2 IP address table. Therefore the
Notification
-- will be associated with the object of the MIB 2 for IP address entry of the
system.

   notifyNCPIPChangeNOTIFICATION-TYPE
      OBJECTS { entPhysicalName,ipAdEntAddr}
      STATUS  current
      DESCRIPTION"Notifies if there is a change in the IP
                address of the NCP."
      ::=  {  nbxNotifications  2  }

-- This notifications is fired when the voicemail ports that are available in the
system get
-- exhausted.
   notifyVoiceMailPortsExhaustedNOTIFICATION-TYPE
      OBJECTS { entPhysicalName,ncpNumberOfVMPorts }
      STATUS  current
      DESCRIPTION"Notifies if the voice mail
              ports get exhausted."
```

```
      ::=  {  nbxNotifications  3  }

-- This notification is fired whenever an administrator fails to logon properly.
-- The object to which this is mapped is the entPhysicalName of the Entity table.

   notifyFailedLogonAttemptNOTIFICATION-TYPE
      OBJECTS { entPhysicalName }
      STATUS  current
      DESCRIPTION"Notifies if there is a Failed logon
                 attempt by the Administrator."
      ::=  {  nbxNotifications  4  }

   notifyVTLConnectionFailureNOTIFICATION-TYPE
      OBJECTS { entPhysicalName}
      STATUS  current
      DESCRIPTION"Notifies if any of the incoming or
                  outgoing VTL calls result in a Failure."
      ::=  {  nbxNotifications  5  }

-- The phone extension is not a table object and therefore the phone name is listed.
-- for the phones and gateways the Device name is associated to the notification
objects
-- so that the manager can get to know the device that sent the notification.
-- By default the notification contains the information on the MAC address of
-- phone, gateway,span,channel as it is the index of the respective table.
   notifyPhoneStatusChangeNOTIFICATION-TYPE
      OBJECTS { phoneStatus,phoneDeviceName }
      STATUS  current
      DESCRIPTION"Notifies if the status of phone
                 changes."
      ::=  {  nbxNotifications  6  }

   notifyPhoneIPChangeNOTIFICATION-TYPE
      OBJECTS { phoneIPAddress,phoneDeviceName }
      STATUS  current
      DESCRIPTION"Notifies  if the IP address of a phone
              changes."
      ::=  {  nbxNotifications  7  }

   notifyGatewayStatusChangeNOTIFICATION-TYPE
      OBJECTS { gatewayStatus,gatewayDeviceName }
      STATUS  current
      DESCRIPTION"Notifies if there is a change in the
              status of the gateway. The gateways include all the boards of
              T1,E1 etc connected to the NBX."
      ::=  {  nbxNotifications  8  }
```

```
   notifyGatewayIPChangeNOTIFICATION-TYPE
      OBJECTS { gatewayIPAddress,gatewayDeviceName }
      STATUS  current
      DESCRIPTION"Notifies if there is a change in the IP
              Address of the gateway,"
      ::=  {  nbxNotifications  9  }

-- The notification gets fired if all the ports get busy in a gateway. The
notification is associated
-- to a mac address so as to inform the user of the device that has fired.

   notifyGatewayAllPortsBusyNOTIFICATION-TYPE
      OBJECTS { gatewayDeviceName,entPhysicalName }
      STATUS  current
      DESCRIPTION"Notifies if all the ports of the
                      Gateway connected to NBX gets busy."
      ::=  {  nbxNotifications  10  }
-- spanstatus notification is associated to its name, so that the manager can know
-- which span has sent that.
   notifySpanStatusChangeNOTIFICATION-TYPE
      OBJECTS { dlcSpanStatus,dlcSpanName }
      STATUS  current
      DESCRIPTION"Notifies if there is a change in the
                                  span status of the Digitl line card"
      ::=  {  nbxNotifications  11  }

   notifyChannelStatusChangeNOTIFICATION-TYPE
      OBJECTS { dlcChannelStatus,dlcChannelName}
      STATUS  current
      DESCRIPTION"Notifies if there is a change in the
                                  channel status of the digital line card."
      ::=  {  nbxNotifications  12  }

-- Notifies if there is a change in the link status of the gateway. The
-- device name is associated to indicate the manager as to which gateway and which
-- link has sent the notification.

   notifyGatewayLinkStateChangeNOTIFICATION-TYPE
      OBJECTS { analogLineStatus,analogLineDeviceName }
      STATUS  current
      DESCRIPTION"Notifies if there is a change in the
                                  status of the line card ports that are
                                  connected to the NBX."
      ::=  {  nbxNotifications  13  }
-- Notifies if any of the license limits are exceeded in a NBX.
```

```
   nbxLicenseLimitThresholdNOTIFICATION-TYPE
      OBJECTS { entPhysicalName,ncpLicenseName }
      STATUS  current
      DESCRIPTION"Notifies if the threshold for the License is exceeded."
      ::=  {  nbxNotifications  14  }

   nbxLicenseAddDeleteNOTIFICATION-TYPE
      OBJECTS {entPhysicalName, ncpLicenseName }
      STATUS  current
      DESCRIPTION"Notifies if a new license is added or deleted"
      ::=  {  nbxNotifications  15  }


END
```

GLOSSARY

A B C D E F G H I J K
L M N O P Q R S T U
V W X Y Z

Symbols

10BASE-T A form of Ethernet and IEEE 802.3 network cabling using twisted pair. It provides 10Mbits/s with a maximum segment length of 100 m (382 ft).

10BASE2 An implementation of IEEE 802.3 Ethernet standard, often called thinnet or cheapernet, because it uses thin coaxial cable. 10BASE2 runs at a data transfer rate of 10 Mbits/s with a maximum segment length of 185 m (607 ft) per segment.

911 The emergency service that provides a single point of contact for police and fire departments. See also E911.

account codes Codes that allow you to keep track of calls associated with a client or account for tracking purposes.

ADSL Asymmetrical Digital Subscriber Line**.** A telephone line that delivers high-speed data services, such as Internet access, videoconferencing, interactive TV, and video on demand. The line is split asymmetrically so that more bandwidth can be used from the telephone company to the customer (downstream) than from the customer to the telco (upstream).

ATM Asynchronous Transfer Mode. A cell-based data transfer technique in which channel demand determines packet allocation. ATM offers fast packet technology, real-time, demand-led switching for efficient use of network resources.

Attendant Console A standard telephony device that shows the status of each extension in a telephone system. The Attendant Console is usually used by a receptionist to connect incoming calls to the correct extension. All

incoming calls ring at the telephone associated with the Attendant Console.

AUI Attachment Unit Interface. The IEEE 802.3-specified cable and connector used to attach single-channel and multiple-channel equipment to an Ethernet transceiver. Defined in Section 7 of the 802.3 standard.

auto dial A feature that opens a line and dials a preprogrammed telephone number.

Auto Attendant A system feature that provides incoming callers with menu options to help them reach the appropriate person or information.

Auto Discovery A feature that "discovers" a new telephone or other device on the network. A new telephone receives a default telephone number that displays on the telephone display panel. A new device is assigned one or more extension numbers or device numbers.

auto redial A modem, fax, or telephone feature that redials a busy number a fixed number of times before giving up.

autorelocation A feature that allows a telephone to keep its extension number and personal and systems settings when you connect it to a different Ethernet jack on the same LAN.

ACD Automatic Call Distribution. A feature that distributes calls to agents and queues the calls that have not been answered before a pre-determined time period expires. The ACD also manages recorded announcements to callers, manages individual ACD agents and groups of agents, and provides database reports on both calls and agents.

B

backbone A high-capacity network that links together other networks of lower capacity. A typical example is a Frame Relay or ATM backbone that serves a number of Ethernet LAN segments.

bandwidth The capacity of a connection method to carry data.

BRI Basic Rate Interface. An ISDN standard that allows two circuit-switched B (bearer) channels of 64 kbps each plus one D (data) channel at 16 kbps for a total of 144 kbps to be carried over a single twisted pair cable.

bridge A networking device that connects two separate local area networks and makes the LANs look like a single LAN, passing data between the networks and filtering local traffic.

bridged extension An extension of a primary telephone that displays on one or more secondary telephones. Incoming calls and indeed any activity associated with the primary telephone can be managed on any of the secondary telephones.

broadcast A simultaneous transmission method that sends each packet from one node to all other nodes.

buffer A temporary storage area for data that compensates for a difference in transmission speeds.

bus topology A type of network in which all devices are connected to a single cable. All devices that are attached to a bus network have equal access to it, and they can all detect all of the messages that are put on to the network.

byte A unit of 8 bits that forms a unit of data. Usually each byte stores one character.

call coverage point The user-specified destination for the call forward feature, that is, how the system is to manage incoming calls when the user is unable to answer the telephone.

C

caller ID A telephone company service that displays the name and number associated with an incoming call. Also called calling line ID or CLI. See also CLIR.

call forward A feature that allows calls to be transferred to a call coverage point (voice mail, the Auto Attendant, or a prespecified telephone number) when the user is unable to answer the telephone.

calling groups A feature that transfers incoming calls to a specified group of telephones. All telephones ring at the same time. See also hunt groups.

call park A feature that places a call in a "holding pattern" and makes it available for others to pick up from any telephone on the system.

call permissions Restrictions that an administrator establishes to control the types of calls that users can place from their telephones. Can be based on time of day.

call pickup A feature that allows users to retrieve calls that ring on other telephones.

Call Processor The device that manages call traffic, voice mail, the Auto Attendant, and related applications in an system.

call reports A feature that downloads data about calls and creates simple reports or exports the data for use in spreadsheets, word processors, or reporting programs.

category 3 The cable standard for UTP (unshielded twisted pair) voice-grade cabling that is specified by EIA/TIA 568 for use at speeds of up to 10Mbit/s, including 10BASE-T Ethernet.

category 4 The cabling standard specified by EIA/TIA 568 for use at speeds of up to 20Mbit/s.

category 5 The cabling standard specified by EIA/TIA 568 for use at speeds of up to 100 Mbit/s including FDDI (TP PMD), 100BASE-T and 100BASE-VG-AnyLan, and potentially ATM at 155Mbit/s.

Channel Service Unit (CSU) Equipment installed on customer premises to terminate a DDS or T1 circuit. CSUs provide network protection and diagnostic capabilities and regenerate the signal received from the network. The CSU also controls pulse shape and amplitude for the transmission of the signal into the network.

client/server computing The division of an application into two parts that are linked by a network. A typical example is a database application in which the database and application software reside on a server, and the interface for entering or retrieving information resides on individual workstations (clients).

CLI See caller ID.

CLIR Calling Line Identity Restriction. A telephone company option that allows the caller to withhold caller identity from the person being called.

coaxial cable High-capacity networking cable that is formed by an outer braided wire or metal foil shield surrounding a single inner conductor, with plastic insulation between the two conducting layers. "Coax" cable is used for broadband and baseband communications networks. Ethernet employs *thin* coaxial cable in 10BASE2 and *thick* cable in 10BASE5.

CODEC **CO**mpressor/**DEC**ompressor. A hardware circuit or software routine that compresses and decompresses digitized audio, video, or image data.

Most codecs include the functions of A/D and D/A conversion as well as compression and decompression.

COder/**DEC**oder. A hardware circuit that converts analog audio or video signals into digital code, and vice versa, using techniques such as pulse code modulation and delta modulation. A CODEC is an A/D and D/A converter.

collapsed backbone Network architecture in which the backplane of a device, such as a hub, performs the function of a network backbone. Example: The backplane routes traffic between desktop nodes and between other hubs serving multiple LANs.

collision The result of two devices on a shared transmission medium, like Ethernet, transmitting simultaneously. Both devices must retry their transmissions. A delay mechanism used by both senders drastically reduces the chances of another collision.

collision detection Ethernet devices detect collisions instantly and attempt to resend. This is the principle on which CSMA/CD (Carrier Sense Multiple Access with Collision Detection) is based and the access control method for Ethernet.

concentrator A central chassis into which various modules, such as bridging, supervisory, and 10BASE-T cards are plugged.

congestion The result of increased network use on a LAN segment. Standard network partitioning practices must be invoked to reduce bottlenecks and maximize throughput speeds on the segment.

contention The method used to resolve which users gain access to crowded bandwidth.

CO Central Office. A telephony term for the telephone company site that houses the PSTN switching equipment.

CoS Class of Service. A collection of calling permissions that are assigned to individual users and govern the times and types of calls these users can make.

CPE Customer Premises Equipment. Telecommunications equipment, including PBX systems and wiring, that is located in a user's premises.

CSU Channel Service Unit. Data transmission equipment to repeat the signal from the carrier and link to CPE. Vendors add value to CSUs by adding performance monitoring and management features.

CTI Computer Telephony Integration. A generic name for the technology that connects computers and telephone systems through software applications.

D

data compression A method of reducing the amount of data to be transmitted by reducing the number of bits needed to represent the information.

delayed ringing Prevents a telephone on a shared line from ringing until the incoming call has rung on other telephones a set number of times.

delayed ringing pattern The definition for the order in which telephones ring and how many times each telephone rings.

demand priority access A method for supporting time-sensitive applications such as video and multimedia as part of the proposed 100BASE-VG standard offering l00Mbit/s over voice-grade UTP cable.

DHCP Dynamic Host Configuration Protocol. A method by which devices are assigned temporary, renewable IP addresses by a server when the devices become active on the network.

DID/DDI Direct Inward Dial/Direct Dialing Inward. A feature that allows outside calls to reach an internal extension without going to an operator or Automated Attendant.

direct mail transfer Transfers a caller directly to another user's voice mail without requiring them to wait through ringing and without interrupting the recipient.

domain A group of nodes on a network that form an administrative entity. A domain can also be a number of servers that are grouped and named to simplify network administration and security.

DSP Digital Signal Processor. A special-purpose CPU tailored to manage complex mathematical functions. A DSP takes an analog signal and reduces it to numbers so its components can be isolated, sampled, and rearranged more easily than in analog form.

DSU/CSU Digital (or Data) Service Unit/Channel Service Unit. A pair of communications devices that connect an in-house line to an external

digital circuit (such as T1 and DDS). It is similar to a modem, but connects a digital circuit rather than an analog circuit.

DTMF Dual Tone Multi-Frequency. A term for push button dialing. The pushed button generates a pair of tones which uniquely identify the button that was pressed.

E911 Enhanced 911. The addition of two features to the standard 911 service: one is ANI (Automatic Number Identification) to identify the person associated with the calling telephone, and the other is ALI (Automatic Location Identification) to identify the physical location of the calling telephone.

E

encapsulation The process of sending data encoded in one protocol format across a network operating a different protocol, where it is not possible or desirable to convert between the two protocols. Also known as protocol tunneling.

error correction A technique to restore data integrity in received data that has been corrupted during transmission. Error correction techniques involve sending extra data. The correct form of the data can be reconstructed from the extra information.

error detection A set of techniques that can be used to detect errors in received data. Parity checking techniques include the use of parity bits, checksums or a Cyclic Redundancy Check (CRC).

Ethernet The most widely used LAN transmission protocol. Based on a network bus topology, it runs at a maximum 10Mbit/s and can use a wide variety of cable types. The IEEE Ethernet standard is IEEE 802.3.

Ethernet switching A technique that brings the advantages of a parallel networking architecture to contention-based Ethernet LANs. Each LAN can be segmented with its own path. When users on different segments exchange data, an Ethernet switch dynamically connects the two separate Ethernet channels without interfering with other network segments.

F

fast Ethernet An evolution of Ethernet that raises the bandwidth to 100 Mbit/s.

fast packet switching A WAN technology for transmitting data, digitized voice, and digitized image information. It uses short, fixed length packets.

FDDI Fiber Distributed Data Interface. An optical fiber-based token-passing ring LAN technology that carries data at a rate of 100 Mbit/s.

FRAD Frame Relay Access Device. A wide-area networking device that forwards traffic to and from the endpoint of a the network.

frame A structured group of bits sent over a link. A frame can contain control, addressing, error detection, and error correction information. The term is often used synonymously with the term packet.

frame relay A packet-switching wide-area technology for interconnecting LANs at high speeds.

G

gateway A network device that provides a means for network traffic to pass from one topology, protocol, or architecture into a different topology, protocol, or architecture.

gigabit Ethernet An Ethernet technology that raises transmission speed to 1 Gbit/s, targeted primarily for use in backbones.

glare A condition in telephony where both ends of an available connection are seized at the same time.

group mailboxes Mailboxes that are not associated with a single telephone but allow a group of users to have joint access to a single mailbox.

H

H.323 An ITU standard for the transmission of real-time audio, video, and data communications over packet-switched networks, such as local area networks (LANs) and the Internet. H.323 is the basis for Internet telephony.

header The control information added to the beginning of a transmitted message. This might consist of packet or block address, destination, message number and routing instructions.

hierarchical network A network with one host at its hub, which is the major processing center, and one or more satellite processing units.

hot swap The ability of a device to have parts removed and replaced without turning off the device and without interrupting the service the device provides.

hub The center of a star topology network or cabling system. A multi-node network topology that has a central multiplexer with many nodes feeding into and through the multiplexer or hub. The nodes do not directly interconnect.

hunt groups Informal "call centers" in which a call rings to one member of the group. If there is not answer, the call rings at the next member's telephone and so on until a member answers.

hybrid mode A PBX operating mode in which some outside lines are grouped together in pools while other lines are assigned directly to buttons on telephones. Users access outside lines by dialing a pool access code. See also key mode.

I

IEEE Institute of Electrical and Electronic Engineers. A U.S. publishing and standards organization responsible for many LAN standards, such as the 802 series.

IEEE 802.2 The Data Link standard for use with IEEE 802.3, 802.4 and 802.5 standards. It specifies how a basic data connection must be set up over the cable.

IEEE 802.3 The Ethernet standard. A physical layer definition that includes specification for cabling plus the method of transmitting data and controlling access to the cable.

IETF Internet Engineering Task Force. The standards-setting body for the Internet. Protocols adopted by the IETF define the structure and the operation of the Internet.

IMAP Internet Message Access Protocol. A method of accessing electronic messages that are kept on a server. IMAP defines how an e-mail program can access messages that are stored on a remote server.

intelligent hub See managed hub.

IP Internet Protocol. The TCP/IP standard protocol that defines the IP datagram as the unit of information passed across an Internet. IP provides the basis for connectionless packet delivery service.

IP address The address used by devices on the network to establish their unique identity. IP addresses are composed of four fields separated by dots. Each field is an 8-bit number (0 through 255). IP addresses can be permanently assigned, or they can be temporarily assigned by DHCP.

IP telephony Technology that allows voice, data, and video to be transmitted over IP-based networks.

ISDN Integrated Services Digital Network. An international telecommunications standard for transmitting voice, video and data over digital lines running at 64 kbps. ISDN uses B channels, or "bearer" channels, to carry voice and data. It uses a separate D channel, or "delta," channel for control signals to the telephone company computer.

ITU International Telecommunication Union. An international standards organization for telecommunications.

J

jitter The variation in latency (waiting time) for different packets on the network. For real time data such as voice transmission, jitter must be kept to a minimum.

K

key mode A telephone system operating model in which each telephone in the system has buttons for each available outside line. Also known as a square plan or a direct system inward access (DISA) system. See also hybrid mode.

L

LAN local area network. A communications system that links computers, printers, and other devices. LANs allow users to communicate and share resources like hard disk storage and printers. Devices linked by a LAN might be on the same floor or within a building or campus.

LAN segment A section of a local area network that is used by a particular workgroup or department and separated from the rest of the LAN by a bridge, router or switch.

LAN switch A network device that connects stations or LAN segments, also known as a frame switch.

latency The sum of all the delays in an end-to-end connection.

layering The process of dividing complex software up into several layers, each of which performs a specific task. Layering allows faster and easier software development and is often used in public, open software.

LCD Liquid Crystal Display. A low cost display technology.

line pool In a PBX system, outside lines are pooled and arbitrated by the Call Processor. To call an outside number, a user must dial the line pool access number, typically 9, and the Call Processor assigns the next available line.

LLC Logical Link Control. A data link protocol for LANs that is part of the IEEE 802.2 standard and common to all LAN standards for OSI model data link, level two transmissions.

loop start The most common signaling method in the public telephone network, typically used for residence and business CO lines.

M

MAC Media Access Control. A sub-layer of the Data Link layer (Layer 2) of the ISO OSI model responsible for media control. Also known as the "MAC layer."

MAC address A unique 48-bit number that is encoded in the circuitry of a device to identify it on a LAN. Also known as a "hardware address" or an "Ethernet address."

managed hub A network device in which each port on the hub can be configured, monitored, and enabled or disabled by a network administrator from a hub management console or utility tied into an SNMP (Signaling Network Management Protocol) platform. Hub management can also include gathering information about network parameters.

MAU Medium Attachment Unit. A transceiver that provides the correct electrical or optical connection between the computer and IEEE 802.3 LAN media.

MIB Management Information Base. A database that can be accessed by a gateway running CMIP (Common Management Information Protocol),

CMOT (CMIP Over TCP/IP), or SNMP (Signaling Network Management Protocol) network management protocols. The MIB defines variables needed by the protocol to monitor and control components in a network. Managers can fetch or store these variables.

modem **MO**dulator/**DEM**odulator. A modem converts a binary bit stream to an analog signal and vice versa.

multiplexer A device that can send several signals over a single line. A similar device at the other end of the link then separates the signals.

multi-tasking The concurrent execution of two or more tasks or the concurrent use of a single program that can carry out many functions.

MWI Message Waiting Indicator. A feature that informs the recipient by means of a lit status light or LCD display panel that the recipient has a pending message.

allows users to send, retrieve, or cancel special indicators that i.

N

NetBEUI NetBios Extended User Interface. A network device driver or transport protocol that is the transport driver supplied with LAN Manager.

NetBios Network Basic Input/Output System. Software developed by IBM that provides the interface between the PC operating system, the I/O bus, and the network. Since its design, NetBIOS has become a de facto standard.

NetWare LAN Network Operating System and related products developed by Novell. NetWare is based on the SPX/IPX networking protocols.

network collisions Result of two stations simultaneously attempting to use a shared transmission medium. See collision.

network congestion Result of increased network utilization. Creates traffic bottlenecks on a LAN segment. See congestion.

network layer Layer 3 in the OSI model responsible for the routing and relaying through one or more networks in multiple link or wide area environments.

network management The process and technique of remotely or locally monitoring and configuring networks.

network ping A packet transfer that checks logical continuity between a PC and a specified IP address.

NIC Network Interface Card. Controller circuitry that connects a node to a network, usually in the form of a card in a PC expansion slot. In conjunction with the NOS (Network Operating System) and PC operating system, it helps transmit and receive messages on the network.

node Device on a network that demands or supplies services. Also, a location where transmission paths are connected.

NOS Network Operating System. Software that connects all the devices on a network so that resources can be shared efficiently and managed from a central location. Novell NetWare is one example of a network operating system.

O

OEM Original Equipment Manufacturer. The maker of a product or component that is marketed by another vendor, integrator, VAR (Value Added Reseller), or reseller.

off-hook The state of a telephone line that allows dialing and transmission but prohibits incoming calls from being answered. The term stems from the days when a telephone handset was lifted off of a hook. Contrast with on-hook.

off-site notification A feature that sends a message to a pager, outside telephone number, or e-mail account that informs a user of a voice mail message. The user can retrieve the messages remotely.

on-hook The state of a telephone line that can receive an incoming call.

OSI model A conceptual model of hardware and software layers that define when, how, and in what order data can be transmitted on a network. The OSI Model defines seven layers:

Layer 7	Application layer
Layer 6	Presentation layer
Layer 5	Session layer
Layer 4	Transport layer
Layer 3	Network layer
Layer 2	Data Link layer

Layer 1 Physical layer

out-of-band signaling An extra signal transmitted with the information signal to monitor and control a transmission. It provides an additional layer of resilience by using a separate channel.

P

packet A collection of bits, including address, data, and control information, that are transmitted together. The terms frame and packet are often used synonymously.

packet buffer Memory space reserved for storing a packet awaiting transmission or for storing a received packet.

packet switching A method of switching data in a network. Individual packets of a set size and format are accepted by the network and delivered to their destination. The sequence of packets is maintained, and destination established, by the exchange of control information (also contained in the packets) between the sending terminal and the network before the transmission starts.

paging 1) A communications service that includes a one-way beeper service, one-way text service, and two-way text and voice service.

2) A public address announcement system. Many PBX telephone systems can do paging through the speakers in the telephone sets.

PBX Private Branch eXchange. An in-house telephone switching system that interconnects telephone extensions to each other, as well as to the outside telephone network. It can include functions such as least cost routing for outside calls, call forwarding, conference calling, and call accounting.

PCS Personal Communications Services. Refers to a variety of wireless services emerging after the U.S. Government auctioned commercial licenses in late 1994 and early 1995.

phantom mailbox A user profile that uses a telephone number with no associated telephone. Messages can be sent to the phantom mailbox from within the voice mail system. The Auto Attendant can route messages to the phantom mailbox, and you can dial the phantom mailbox directly.

port A computer interface capable of attachment to another device, such as a modem for communicating with a remote terminal or, if the port is within a hub, to a workstation.

POTS Plain Old Telephone Service.

PPP Point-to-Point Protocol. An addition to the Internet protocol suite to help connect devices where dissimilar transport protocols exist. Typically used for serial connections to the Internet.

predictive dialing Automated dialing feature in which CTI software predicts when you will end your current call, and dials the next call in advance.

pretranslator A device that interprets and modifies a sequence of incoming digits or transmits outgoing digits.

preview dialing Automated dialing feature in which CTI software queues the next call to be made but allows you to check and activate the call.

PRI Primary Rate Interface. An ISDN service for users with large bandwidth requirements, such as large PBX systems or high performance video desktop conferencing systems; the ISDN equivalent of a T1 circuit.

protocol A set of rules governing the information flow within a communications infrastructure. A protocol typically specifies the structure of parameters like format, timing, and error correction.

protocol converter A device that translates between two protocols to facilitate communications between different computers or different systems.

PSTN Public-Switched Telephone Network. The term describes the national telephone network.

punch-down block Telephony term describing the connector arrangements for distributing and connecting unshielded and shielded twisted pair wiring inside a building. Typically found in telephone wiring closets.

Q

Q.921/931 ITU-TS "Q Series" Recommendations describing Lap-D, the Layer 2 protocol for an ISDN D-channel. See OSI model.

R

reconfiguration The process of physically altering the location or functionality of network or system elements. Automatic configuration describes the way sophisticated networks can readjust themselves in the event of a link or device failing, enabling the network to continue operation.

redundancy In data transmission, this refers to characters and bits that can be removed from a transmission without affecting the message. In data processing and data communications, it means providing backup for components so that if one of them fails, the system continues to run without interruption.

REN Ringer Equivalency Number. A number that indicates how much power is required by a telephone to make it ring. When connecting telephones to a telephone line, the sum of the RENs of the telephones must be less than the rated REN capacity of the telephone line.

repeater A device that extends the maximum length of cable that can be used in a single network.

RMON Remote Monitoring. A facet of SNMP-based network management, the RMON MIB (Management Information Base) defines the standard network monitoring functions for communication between SNMP-based management consoles and remote monitors. A typical MIB captures information about a device, but RMON captures information about traffic between devices.

RJ-11 A four-wire modular connector used by the telephone system.

RJ-45 An eight-wire modular connector used by telephone systems. The eight-pin modular connectors used for 10BASE-T UTP cable resemble RJ-45 connectors, but they have substantially different electrical properties.

router A network device that links LANs together locally or remotely as part of a WAN. A network built using routers is often termed an internetwork.

routing The process of delivering a packet across one or more networks via the most appropriate path.

SA System Appearance

S

screen POP A CTI term for a window that automatically opens on a user's computer when a predefined telephone event occurs. For example, an incoming call could generate a screen pop that lists caller ID information.

segment A LAN term meaning an electrically continuous piece of the bus. Segments can be joined together using repeaters or bridges.

serial interface Hardware for sending and receiving data one bit at a time.

SMDR Station Message Detail Recording. A stream of call data from the telephone system. Typically, the data is not stored on the telephone system itself. Rather, it is captured by an external device that connects to the telephone system through an RS232 port.

SMTP Simple Mail Transfer Protocol. The TCP/IP standard protocol for transferring electronic mail messages from one machine to another. SMTP specifies how two mail systems interact and the format of control messages they exchange to transfer mail.

SNA Systems Network Architecture. IBM's layered communications protocol for sending data between IBM hardware and software.

STP Shielded Twisted Pair. A twisted pair of wires surrounded by a shield that is typically made of braided wire or metal foil.

Supervisory Monitoring A facility that allows a supervisor to monitor incoming calls to agents while those calls are in progress.

switched Ethernet An Ethernet network that allows each user the full Ethernet bandwidth of 10 Mbit/s to another node.

system-wide greetings A special type of time-dependent greeting that is used throughout the system.

T

T1/E1 A high-speed data channel that can manage 24 voice or data channels (T1) or 30 voice or data channels (E1) at 64Kbit/s. Refers to the U.S. T1 line or European E1 equivalent.

T3 A U.S. standard for high-speed data transmission at 44.736 Mbit/s, providing the equivalent bandwidth of 28 T-1 circuits. The carrier channel can manage 672 voice or data channels.

TAPI Telephony Applications Programming Interface

A Microsoft Windows standard interface for integration between telephone systems and Windows-based software. A typical example is integrating Caller ID with a database on your computer that contains detailed information about potential callers. When your telephone rings, a window displays on your computer with information about the caller.

TCP/IP Transmission Control Protocol/Internet Protocol. The suite of protocols that define how to move information over the Internet.

thin Ethernet An 802.3 LAN that uses smaller than normal diameter coaxial cable; often used to link PCs together. Also known as 10BASE2.

time-dependent greeting Greetings that usually indicate the time of day that the caller is calling (morning, afternoon, evening) and are an optional feature of the Automated Attendant.

toll-free The U.S. term for "free phone."

toll restrictions The U.S. term for "call barring."

translation The process of interpreting or modifying dialed digits for incoming or outgoing calls and allows the call to progress through the network.

trunk A communications channel between two points. It often refers to large-bandwidth telephone channels between major switching centers, capable of transmitting many simultaneous voice and data signals.

twisted pair Two insulated wires twisted together with the twists varied in length to reduce potential signal interference between the pairs. Twisted pair is the most common medium for connecting telephones, computers and terminals.

U

UPS Uninterruptible Power Supply. A secondary power source attached to a piece of hardware, for example a server, which provides backup power for conducting an orderly shutdown if the server's normal power supply fails.

UTP Unshielded Twisted Pair. Two insulated wires twisted together with the twists varied in length to reduce potential signal interference between the

pairs. The standard cabling used for telephone lines and Ethernet 10BASE-T.

V

virtual LAN A logical, rather than a physical, LAN that includes workgroups drawn together for business reasons or for a particular project regardless of the location of the members.

VPIM Voice Profile for Internet Mail. A set of Internet protocols that merges voice messaging and e-mail. VPIM lets voice mail and e-mail servers exchange messages across TCP/IP-based intranets and the Internet.

VTL Virtual Tie LIne. Allows several domains to create tie lines on demand and to place calls over a WAN. Uses peer-to-peer connections for the audio.

W

WAN Wide Area Network. A network that covers a larger geographical area than a LAN. In a WAN, telecommunications links are normally leased from the appropriate Public Telephone Operator (PTO).

wiring closet The location, usually a physical box, in which the cabling on one floor of a building is terminated.

workstation Another name for a computer, typically running UNIX or the Windows NT operating system.

INDEX

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

3Com Corporation LIMITED WARRANTY

Replace this text with your Product Name

HARDWARE

3Com warrants this hardware product to be free from defects in workmanship and materials, under normal use and service, for the following length of time from the date of purchase from 3Com or its authorized reseller:

3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or if neither of the two foregoing options is reasonably available, 3Com may, in its sole discretion, refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. 3Com warrants any replaced or repaired product or part for ninety (90) days from shipment, or the remainder of the initial warranty period, whichever is longer.

SOFTWARE

3Com warrants that each software program licensed from it will perform in substantial conformance to its program specifications, for a period of ninety (90) days from the date of purchase from 3Com or its authorized reseller. 3Com warrants the media containing software against failure during the warranty period. No updates are provided. 3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to refund the purchase price paid by Customer for any defective software product, or to replace any defective media with software which substantially conforms to applicable 3Com published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty or representation that its software products will meet Customer's requirements or work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a "bug" or defect in the third party's product or from use of the software product not in accordance with 3Com's published specifications or user manual.

YEAR 2000 WARRANTY

In addition to the Hardware Warranty and Software Warranty stated above, 3Com warrants that each product sold or licensed to Customer on and after January 1, 1998 that is date sensitive will continue performing properly with regard to such date data on and after January 1, 2000, provided that all other products used by Customer in connection or combination with the 3Com product, including hardware, software, and firmware, accurately exchange date data with the 3Com product, with the exception of those products identified at 3Com's Web site, tap://www.3com.com/products/yr2000.html, as not meeting this standard. If it appears that any product that is stated to meet this standard does not perform properly with regard to such date data on and after January 1, 2000, and Customer notifies 3Com before the later of April 1, 2000, or ninety (90) days after purchase of the product from 3Com or its authorized reseller, 3Com shall, at its option and expense, provide a software update which would effect the proper performance of such product, repair such product, deliver to Customer an equivalent product to replace such product, or if none of the foregoing is feasible, refund to Customer the purchase price paid for such product.

Any software update or replaced or repaired product will carry a Year 2000 Warranty for ninety (90) days after purchase or until April 1, 2000, whichever is later.

OBTAINING WARRANTY SERVICE

Customer must contact a 3Com Corporate Service Center or an Authorized 3Com Service Center within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase from 3Com or its authorized reseller may be required. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid and packaged appropriately for safe shipment, and it is recommended that they be insured or sent by a method that provides for tracking of the package. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after 3Com receives the defective product.

Dead- or Defective-on-Arrival. In the event a product completely fails to function or exhibits a defect in materials or workmanship within the first forty-eight (48) hours of installation but no later than thirty (30) days after the date of purchase, and this is verified by 3Com, it will be considered dead- or defective-on-arrival (DOA) and a replacement shall be provided by advance replacement. The replacement product will normally be shipped not later than three (3) business days after 3Com's verification of the DOA product, but may be delayed due to export or import procedures. When an advance replacement is provided and Customer fails to return the original product to 3Com within fifteen (15) days after shipment of the replacement, 3Com will charge Customer for the replacement product, at list price.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com for repair, whether under warranty or not.

WARRANTIES EXCLUSIVE

IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO OPEN, REPAIR OR MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OTHER HAZARDS, OR ACTS OF GOD.

LIMITATION OF LIABILITY

TO THE FULL EXTENT ALLOWED BY LAW, 3COM ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

DISCLAIMER

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

GOVERNING LAW

This Limited Warranty shall be governed by the laws of the State of California, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

3Com Corporation
5400 Bayfront Plaza
Santa Clara, CA 95054
(408) 326-5000

FCC CLASS A VERIFICATION STATEMENT

WARNING: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules, and the Canadian Department of Communications Equipment Standards entitled, "Digital Apparatus," ICES-003. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful

interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at the user's own expense.

Changes or modifications not expressly approved by 3Com could void the user's authority to operate this equipment.

FCC Class B Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1 This device may not cause harmful interference, and

2 This device must accept any interference received, including interference that may cause undesired operation.

WARNING: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules, and the Canadian Department of Communications Equipment Standards entitled, "Digital Apparatus," ICES-003. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from the one which the receiver is connected to.
- Consult the dealer or an experienced radio/TV technician for help.

The user may find the following booklet prepared by the Federal Communications Commission helpful:

The Interference Handbook

This booklet is available from the U.S. Government Printing Office, Washington, D.C. 20402. Stock No. 004-000-00345-4.

NOTE: In order to maintain compliance with the limits of a Class B digital device, 3Com requires that you use quality interface cables when connecting to this device. Changes or modifications not expressly approved by 3Com could void the user's authority to operate this equipment. Refer to the manual for specifications on cabling types.

FCC Declaration of Conformity

We declare under our sole responsibility that the

Model:	**Description:**
3CXXX	Product Name

to which this declaration relates, is in conformity with the following standards or other normative documents:

- ANSI C63.4-1992 Methods of Measurement
- Federal Communications Commission 47 CFR Part 15, subpart B
  15.107 (a) Class B Conducted Limits
  15.109 (a) Class B Radiated Emissions Limits
- 15.107 (e) Class B Conducted Limits
  15.109 (g) Class B Radiated Emissions Limits

3Com Corporation, 5400 Bayfront Plaza, P.O. Box 58145, Santa Clara, CA 95052-8145